TU WIEN Informatics

Sicherheit von VANETs mit Fokus auf Black Hole Attacks in ETSI C-ITS

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering & Internet Computing

eingereicht von

Daniel Ostovary, BSc
Matrikelnummer 01226423

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuer: Thomas Grechenig
Mitwirkender: Florian Fankhauser

Wien, 9. Juli 2020

Unterschrift Verfasser

Unterschrift Betreuer

TU WIEN Informatics

Security of VANETs with a Focus on Black Hole Attacks in ETSI C-ITS

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Software Engineering & Internet Computing

by

Daniel Ostovary, BSc
Registration Number 01226423

to the Faculty of Informatics

at the TU Wien

Advisor: Thomas Grechenig
Assistance: Florian Fankhauser

Vienna, 9th July, 2020

Signature Author

Signature Advisor

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Sicherheit von VANETs mit Fokus auf Black Hole Attacks in ETSI C-ITS

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering & Internet Computing

eingereicht von

Daniel Ostovary, BSc
Matrikelnummer 01226423

ausgeführt am
Institut für Information Systems Engineering
Forschungsbereich Business Informatics
Forschungsgruppe Industrielle Software
der Fakultät für Informatik der Technischen Universität Wien

Betreuer: Thomas Grechenig
Mitwirkender: Florian Fankhauser

Wien, 9. Juli 2020

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Erklärung zur Verfassung der Arbeit

Daniel Ostovary, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 9. Juli 2020

Daniel Ostovary

Kurzfassung

Das European Telecommunications Standards Institute (ETSI) hat einen Vehicular Ad Hoc Network (VANET)-Standard etabliert – den Cooperative Intelligent Transport Systems (C-ITS)-Standard. Dieser Standard enthält Sicherheitsmaßnahmen um die IT-Sicherheit von Fahrzeugen zu gewährleisten. Black Hole Attacks sind Angriffe auf ETSI C-ITS. In Black Hole Attacks absorbieren Angreifer Pakete und verwerfen diese, um einen Denial-of-Service (DoS) zu verursachen. Da Black Hole Attacks Routing-Protokolle angreifen, ist das Routing-Protokoll von ETSI C-ITS, das GeoNetworking-Protokoll, diesbezüglich besonders relevant.

Diese Diplomarbeit verbessert den aktuellen Forschungsstand im Bereich von Black Hole Attacks auf Mobile Ad Hoc Networks (MANETs)/VANETs. Diese Verbesserung wird durch das Formalisieren einer Definition von Black Hole Attacks und durch das Identifizieren von Eigenschaften, die für die IT-Sicherheit gegen Black Hole Attacks relevant sind, erzielt (z. B. Verhältnis von Angreifer/Netzknoten). Weiters wird in dieser Diplomarbeit eine Risikoanalyse von Black Hole Attacks auf jeden Weiterleitungsalgorithmus des GeoNetworking-Protokolls durchgeführt. Das Ergebnis dieser Analyse ist, dass Black Hole Attacks ein kritisches Risiko für Greedy Forwarding (GF) und Contention-Based Forwarding (CBF) darstellen, falls diesbezüglich keine Sicherheitsmaßnahmen im Einsatz sind. Mit den Sicherheitsmaßnahmen aus dem ETSI C-ITS Standard können Black Hole Attacks auf GF und CBF großteils verhindert werden. Diese Diplomarbeit enthält außerdem einen Auswahlprozess für ein ETSI C-ITS-Simulationsframework und führt wichtige vorläufige Entwicklungen für die Durchführung von Black Hole Attack-Simulation in ETSI C-ITS durch. Die Kombination aus der ETSI C-ITS-Implementierung *Vanetza* und dem Simulator *Objective Modular Network testbed in C++ (OMNet++)* wird als geeignetes Simulationsframework identifiziert. Dieses Simulationsframework wird durch das Luxembourg SUMO Traffic (LuST)-Szenario, einem realistischen Verkehrsdatensatz in urbanem Umfeld, und Funktionalität zur Ermöglichung von Black Hole Attacks erweitert. Die entwickelte Black Hole Attack-Funktionalität enthält Funktionalität zum Verwerfen von GF-/CBF-Paketen und Funktionalität, um GF/CBF global zu forcieren.

Schlüsselwörter

IT Sicherheit, VANET, Black Hole Attack, C-ITS, Risikoanalyse, Simulation

Abstract

The European Telecommunications Standards Institute (ETSI) has established a Vehicular Ad Hoc Network (VANET) standard set – the Cooperative Intelligent Transport Systems (C-ITS) standard set. This standard set contains security standards that shall provide IT security in ETSI C-ITS. One topic in the field of ETSI C-ITS security is black hole attacks. During a black hole attack, an attacker absorbs packets and drops the received packets, leading to a Denial-of-Service (DoS). As black hole attacks are attacks on routing protocols, the routing protocol of ETSI C-ITS is of particular interest. ETSI C-ITS' routing protocol is called *GeoNetworking* protocol.

This thesis improves the understanding of black hole attacks in Mobile Ad Hoc Networks (MANETs)/VANETs by formalizing a definition of black hole attacks and by identifying properties that are relevant for the IT security of MANETs/VANETs against black hole attacks (e.g., the attacker/node ratio or the nodes' speed). Furthermore, this thesis provides a risk analysis of black hole attacks on each forwarding algorithm of the *GeoNetworking* protocol. In this risk analysis, it is found that the Greedy Forwarding (GF) algorithm and the Content-Based Forwarding (CBF) algorithm of the GeoNetworking protocol are under critical risk of black hole attacks if no security measures are taken. As soon as security measures described in the ETSI C-ITS security standards are deployed, the risk of black hole attacks on GF and CBF is mostly prevented. Lastly, this thesis contains a selection process of an ETSI C-ITS simulation framework and provides important preliminary work to enable black hole attack simulations for ETSI C-ITS. The ETSI C-ITS implementation *Vanetza* is identified to be well suited for the simulation of black hole attacks in ETSI C-ITS. Together with the Objective Modular Network testbed in C++ (OMNet++), Vanetza constitutes a simulation framework for ETSI C-ITS. This simulation framework is extended by the Luxembourg SUMO Traffic (LuST) data set, a realistic data set in an urban area, and functionality to enable black hole attacks. The developed functionality is comprised of functionality to drop GF and CBF packets and functionality to enforce either GF or CBF globally.

Keywords

IT Security, VANET, Black Hole Attack, ETSI C-ITS, Risk Analysis, Simulation

Contents

CHAPTER 1

Introduction

This chapter outlines the problem description, motivation, goal, and structure of this thesis.

1.1 Problem Description

Accompanying a trend of connecting everyday items, vehicles are becoming increasingly interconnected through wireless short-range communication. Due to their interconnection they can minimize various traffic-related problems (e.g., traffic accidents, high fuel costs, or difficult navigation), which makes them appear intelligent [Men+18, pp. 24-25]. Hence the name Smart Vehicles [Men+18, pp. 24-25].

The ongoing development in the field of Smart Vehicles is expected to bring multiple improvements to the driving experience including reduced fuel costs, increased road safety, and easier navigation in the near future. To achieve these improvements, along their itinerary Smart Vehicles are planned to communicate with a wide range of device types (e.g., Smart Vehicles, smartphones, or infrastructure units) in close proximity. Smart Vehicles are the central element in this kind of communication. Due to the range of device types and the centrality of Smart Vehicles, this communication is referred to as Vehicle-to-Anything (V2X) communication [Ham+15]. V2X communication is projected to mainly include Smart Vehicles, pedestrian-held devices (e.g., smartphones), and infrastructure units deployed along the roadside.

V2X communication occurs in Vehicular Ad Hoc Networks (VANETs). VANETs can be described as rapidly changing networks supporting a wide range of device types that exchange a vast amount of time- and safety-critical information. Communication systems with such features are relatively new and have not widely been deployed. As a result, VANETs face many challenges related to the establishment of new technology with the aforementioned properties. Some major challenges for their establishment are (1) planning

for upcoming functionality [Cha16], (2) scalability [Cha16], (3) managing the system's complexity [Men+18, p. 15], and (4) providing IT security to ensure safety [Cha16].

The challenges (3) and (4) make current VANETs particularly prone to attacks from cyber adversaries. Historically, complexity and safety-criticality have lead to critical attacks with significant impact, as exemplified by Chodhury and Zulkernine [CZ10] and Farwell and Rohozinski [FR11]. To minimize the risk of similar attacks in VANETs, thorough planning and research are required for VANETs and their security.

VANET standard sets have been established in different regions of the world. In Europe, the European Telecommunications Standards Institute (ETSI) has developed the ETSI Cooperative Intelligent Transport Systems (C-ITS) standard set, while the U.S., Canada, and Japan have adopted their own standard sets [Men+18, p. 5].

ETSI C-ITS defines security standards to provide a secure VANET. However, the ETSI C-ITS' security is neither well-analyzed nor well-tested in current research. Without comprehensive IT security analyses and tests, it is difficult to measure the overall IT security of ETSI C-ITS. This lack of certainty in such a safety-critical field might hinder the adoption of ETSI C-ITS, and consequently the adoption of Smart Vehicles, due to safety concerns of public and private stakeholders.

One major topic within the IT security of ETSI C-ITS is network security. As discussed by Gohkhale et al. [Gok+11], security research in the field of VANETs has shown various attacks on the network layer of VANETs (e.g., flooding attacks or replay attacks). As the risk of such attacks differs between specific VANETs, the risk of attacks on ETSI C-ITS is not clear. One attack with an uncertain risk on ETSI C-ITS is the black hole attack. Black hole attacks are discussed by Deng et al. [Den+02], Baiad et al. [Bai+16], and Tseng et al. [Tse+18]. In this type of attack, an attacker absorbs packets and drops the received packets instead of forwarding them, leading to a Denial-of-Service (DoS).

Black hole attacks target the network layer of a VANET, more specifically the employed network protocol. In ETSI C-ITS this protocol is called the GeoNetworking protocol. The GeoNetworking protocol specifies different forwarding algorithms. As some of these forwarding algorithms function significantly different from each other, the risk of black hole attacks is expected to differ between these forwarding algorithms. Currently, the risk of black hole attacks on each individual GeoNetworking protocol's forwarding algorithm is unclear.

1.2 Motivation

Most current research focuses on either VANETs as a whole or ETSI C-ITS exclusively, which makes recognizing similarities and differences between VANETs as a whole and ETSI C-ITS difficult. To address this problem, this thesis covers VANETs, ETSI C-ITS, and their relation. This provides significant value for further research in both of these fields.

In current research black hole attacks in VANETs are discussed in various settings (e.g., in a cooperative setting by Tamilselvan and Sankaranarayanan [TS08], in a setting with low attacker/Smart Vehicle ratio by Esmaili et al. [Esm+11], or in a setting with security mechanisms against black hole attacks by Ramaswamy et al. [Ram+03]). To researchers in this field and related fields (e.g., the overall security in VANETs) it is likely unclear which of these settings are relevant for the security of black hole attacks in VANETs. An identification and summary of security-relevant properties of black hole attacks on VANETs would address this unclarity.

The network layer security of VANETs is widely discussed in current research (e.g., Hamida et al. [Ham+15], Bittl [Bit17], or Chaubey [Cha16]). In contrast, the network layer security of ETSI C-ITS is rarely discussed beyond the listing of security specifications and recommendations given by ETSI C-ITS. A risk analysis of black hole attacks would lay a foundation in the field of network security in ETSI C-ITS. More research in the field of network security in ETSI C-ITS would allow developers of ETSI C-ITS applications to assess the security of their applications and to adapt their applications to increase security. On this foundation, further research could be based to create an increasingly comprehensive picture of the network security of ETSI C-ITS.

As no publicly available ETSI C-ITS simulation framework (i.e., an ETSI C-ITS implementation integrated into a VANET simulator) currently supports the simulation of black hole attacks, developers of ETSI C-ITS applications have no publicly available means to test the security of their applications against black hole attacks. As a result, it is likely to be difficult for developers to improve the security of their applications. Enabling simulations of black hole attacks in a publicly available ETSI C-ITS implementation would make it easier for developers to test and improve the security of their applications. Enabling such simulations in a realistic traffic scenario would allow developers to easily test the security of their applications with relatively high realism. Furthermore, with the enabling of simulations of black hole attacks in a realistic traffic scenario, ETSI C-ITS security researchers could easily conduct performance analyses of black hole attacks on ETSI C-ITS with additional security measures with relatively high realism. Such follow-up performance analyses would provide first measures of the impact of black hole attacks in ETSI C-ITS.

1.3 Goal

The first goal of this thesis is to identify properties relevant for the security of black hole attacks on Mobile Ad Hoc Networks (MANETs) and apply this knowledge to VANETs.

The second goal of this thesis is to analyze the risk of black hole attacks on the GeoNetworking protocol and to analyze the influence of ETSI C-ITS' network security measures. Such an analysis requires comprehensive studies of the ETSI C-ITS specifications. In the analysis, each forwarding algorithm is analyzed for its robustness against black hole attacks. Subsequently, the security benefits of ETSI C-ITS' security measures against

black hole attacks are examined. The employed risk analysis method follows ETSI Technical Specification (TS) 102 165-1 version 4.2.3 [Ins11a].

The third goal of this thesis is to enable black hole attack simulations in a realistic traffic scenario in ETSI C-ITS. This goal requires setting up an ETSI C-ITS simulation framework with a data set that uses a realistic traffic scenario. To choose the best publicly available ETSI C-ITS implementation, selection criteria are defined. ETSI C-ITS implementations are evaluated and selected, based on this criteria. As there is currently no publicly available ETSI C-ITS implementation that supports black hole attacks, the functionality of the selected ETSI C-ITS implementation is extended with the goal of enabling black hole attack simulations. The conducted extension is documented for traceability and replicability. Subsequently, the selected implementation is integrated into a suitable VANET simulator, making an ETSI C-ITS simulation framework. Then, a data set that uses a realistic and complex traffic scenario is integrated into the ETSI C-ITS simulation framework.

While the identification and derivation of security-relevant properties and the analysis of the risk of black hole attacks are purely theoretical, enabling the simulation of black hole attack scenarios in a realistic traffic scenario consists of theoretical as well as practical elements.

1.4 Thesis Structure

In *chapter 2* the fundamentals of IT security are covered. These fundamentals are required to understand the security aspects of this thesis. After discussing security in IT systems, this chapter goes on to discuss several well-known IT security concepts. Later, measures to achieve IT security are described.

Chapter 3 contains the fundamentals of Intelligent Transport Systems (ITS). As ITS is an umbrella term, the chapter explains the most relevant related terms, such as Smart Vehicles, Vehicle-To-Anything communication, and ITS applications. Consecutively, VANETs and their International Organization for Standardization/Open System Interconnection (ISO/OSI) protocol stack model are described.

Chapter 4 gives an overview of ETSI C-ITS. The chapter consists of the most relevant standards of ETSI C-ITS in each ISO/OSI layer. In particular, the network layer and the security layer of ETSI C-ITS are discussed extensively.

In *chapter 5* the security of VANETs with a special focus on the security of their network layer is examined. Security requirements in VANETs and related challenges are discussed. This discussion is followed by miscellaneous security challenges in VANETs and a list of attacks on the network layer of VANETs. Notably, in this list black hole attacks are missing. Black hole attacks are discussed in the subsequent chapter.

Chapter 6 covers black hole attacks in MANETs and VANETs. After providing a definition of black hole attacks, security-relevant properties are identified. For MANETs, security-relevant properties can be inferred from previous work in this field. VANETs inherit these

security-relevant properties from MANETs. The security-relevant property *robustness of the employed routing protocol* is later assessed for the GeoNetworking protocol in *Chapter 7*.

In *chapter 7* the robustness of the GeoNetworking protocol against black hole attacks is assessed by analyzing the robustness of each forwarding algorithm of the GeoNetworking protocol. Subsequently, based on these robustness analyses, a risk analysis of black hole attacks on each forwarding algorithm is conducted. These risk analyses consider ETSI C-ITS without and with additional ETSI C-ITS security measures.

Chapter 8 describes enabling black hole attack simulations in ETSI C-ITS. Selection criteria for ETSI C-ITS implementations are defined, a selection process of ETSI C-ITS implementations is conducted, the stack of the selected implementation is described, and the selected ETSI C-ITS implementation is set up in a suitable VANET simulator. The selected ETSI C-ITS implementation is extended with the goal of enabling black hole attack simulations in ETSI C-ITS. Later, selection criteria for data sets are defined and the most fitting data set for this thesis is selected. The selected data set is integrated into the ETSI C-ITS implementation and the VANET simulator.

Chapter 9 provides an overview of work related to VANETs, ETSI C-ITS, and black hole attacks. As VANETs and ETSI C-ITS are fairly broad topics, only selected related topics are presented here. These topics include the U.S. American counterpart to ETSI C-ITS *Wireless Access in Vehicular Environments* (WAVE), traditional vehicular security, and even more strongly related topics, such as the cost of traffic accidents and security measures in VANETs and ETSI C-ITS.

Chapter 10 summarizes the findings of this thesis, provides a discussion of the findings and an outlook on future work. The findings are divided into two parts: findings on black hole attacks on MANETS, VANETs, and ETSI C-ITS and findings on the simulation of black hole attacks in ETSI C-ITS. Several ideas for future work are presented.

Chapter 11 concludes the work in this thesis.

CHAPTER 2

Fundamentals of IT Security

To understand this thesis, a general understanding of IT security is required. This chapter provides such an understanding by describing well-known security properties, widely-used security primitives, and measures to achieve the aforestated security properties.

2.1 Security in IT Systems

Firstly, it is necessary to define the term *security in IT systems*. There are multiple definitions of this term. This thesis will rely on the definition of the National Institute of Standards and Technology (NIST).

The National Institute of Standards and Technology Interagency/Internal Report (NISTIR) 7298 Revision 2 [Kis13] defines security in IT systems as follows:

> Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

The security properties of this definition – confidentiality, integrity, and availability – are commonly referred to as the Confidentiality, Integrity, and Availability Triad (CIA Triad). [Sta+18, p. 25]

2.1.1 Security Properties Triad

The properties of the CIA Triad are defined as follows [Sta+18, p. 25]:

- Confidentiality – The confidentiality property forbids unauthorized access to information. Confidentiality consists of two related concepts: Data confidentiality and Privacy. The difference between these concepts is discussed later in this subsection. [Sta+18, p. 25]

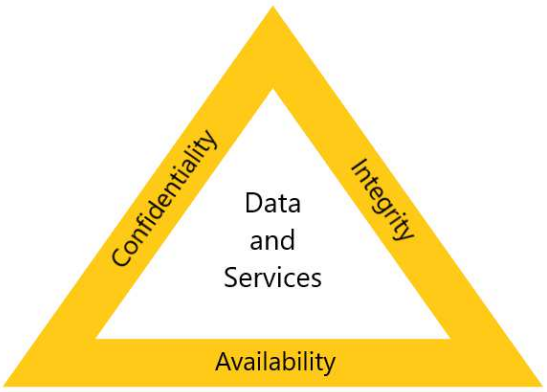


Figure 1: CIA Triad [Sta+18, p. 25]

- Integrity – The integrity property forbids unauthorized modification of data or systems. Integrity consists of two related concepts: data integrity and system integrity. Data integrity ensures that information and programs are only changed in a specified manner by authorized parties. System integrity ensures that a system performs its intended function, free from intended or unintended unauthorized modifications to the system. [Sta+18, p. 25]
- Availability – The availability property requires information to be accessible by authorized parties in a reliable and timely manner. [Sta+18, p. 25]

Figure 1 shows the *CIA Triad* concept.

Traditional integrity definitions, such as the one given by Stallings et al. [Sta+18, p. 25], are not necessarily sufficient for Vehicular Ad Hoc Networks (VANETs). In VANETs, sensor tampering is a widely-known threat (e.g., Amoozadeh et al. [Amo+15] or Chaubey [Cha16]). For the later discussion of integrity in VANETs, the integrity definition given by Stallings et al. is extended by the definition of correctness of content by Biskup [Bis09, p. 41]. Biskup states that data content typically refers to information in the real world. The correctness of data content with respect to the real world can be referred to as correctness of content. For example, wind speed data coming from a wind sensor should reflect the speed of the wind in the real world. If the wind speed data correctly reflects the real-world wind speed, the wind speed data fulfills correctness of content.

2.1.2 Distinction between Data Confidentiality and Privacy

Data confidentiality and privacy are very similar security properties, as they both prevent unauthorized access to information. In current research, these concepts are often not distinguished in detail (e.g., Katz and Lindell [KL14] or Stallings et al. [Sta+18, p. 25]). However, in VANETs the requirements for data confidentiality and the requirements for

privacy differ significantly [Bit17]. As a result, they need to be distinguished in detail in this thesis.

Data confidentiality is frequently argued with two goals (e.g., Bellare et al. [Bel+98], Bellare and Namprempre [BN00], or Katz and Lindell [KL14, pp. 276-278]): INDistinguishability of encryptions (IND), formalized by Goldwasser and Micali [GM84], and Non-Malleability (NM), formalized by Dolev et al. [Dol+91].

IND formalizes an attacker's inability to obtain any information about a plaintext X from a corresponding ciphertext Y. NM formalizes an attacker's inability to generate a ciphertext Y' given a ciphertext Y ($Y \neq Y'$) such that the corresponding plaintexts X and X' are *meaningfully related*. [Bel+98]

Data confidentiality is often described under three attack models (e.g., Bellare et al. [Bel+98], Bellare and Namprempre [BN00], or Dolev et al. [Dol+91]): the chosen plaintext attack (CPA) model, the non-adaptive Chosen Ciphertext Cttack (CCA) model, formalized by Naor and Yung [NY90], and the adaptive Chosen Ciphertext Attack (CCA2) model, formalized by Rackoff and Simon [RS91].

Under CPA, an attacker can obtain a ciphertext of arbitrary plaintexts. Under CCA, in addition to obtaining ciphertexts of arbitrary plaintexts, an attacker can obtain plaintexts of arbitrary ciphertexts from a decryption oracle. The access to this decryption oracle is limited to the time before the challenge ciphertext is obtained. Under CCA2, an attacker has the same capabilities as under CCA, but the attacker may even use the decryption oracle after the challenge ciphertext is obtained. However, the attacker may not ask for the decryption of the challenge ciphertext itself. [Bel+98]

Mixing the goals and attack models six notions of cryptographic security arise: IND-CPA, IND-CCA, IND-CCA2, NM-CPA, NM-CCA, NM-CCA2. [Bel+98]

Privacy assures that parties control or influence what information related to them may be collected and stored and by whom and with whom that information is shared. [Sta+18, pp. 614-615]

Privacy breaks down into four properties [Sta+18, pp. 614-615]:

- Anonymity – Ensures that a party can access a system without disclosing its identity. In particular, this means no party can identify other parties by any means. [Sta+18, pp. 614-615]

  Anonymity is usually argued in an anonymity set (e.g. Pfitzmann and Köhntopp [PK01], Pfitzmann and Hansen [PH10], Diaz et al. [Dia+02], Golle and Partridge [GP09], or Serjantov and Danezis [SD02]). An anonymity set is the set of all possible subjects (e.g. the users of an IT system) [PH10]. Pfitzmann and Hansen [PH10] define anonymity as the state of not being identifiable within an anonymity set.

- Pseudonymity – Ensures that a party can access a system without disclosing its identity to other parties using the system, while still being able to be held accountable for their actions. [Sta+18, pp. 614-615]
- Unlinkability – Ensures that a party can access a system multiple times without other parties being able to link these usages. [Sta+18, pp. 614-615]
- Unobservability – Ensures that a party can access a system without other parties, particularly third parties, being able to detect that the system has been accessed. [Sta+18, pp. 614-615]

2.1.3 Further Security Properties

While the *CIA Triad* is a widely-accepted concept within the field of IT security, it does not provide complete coverage (e.g., it does not cover accountability). As a result, it is sometimes extended by additional properties. [Sta+18, pp. 25-26]

Two of the most common additional properties are [Sta+18, pp. 25-26]:

- Authenticity – The authenticity property requires a party to be genuine and verifiable. Authenticity provides confidence in the validity of a transmission, a message, or a message originator. [Sta+18, pp. 25-26]
- Accountability – The accountability property requires actions to be traceable to the party that has performed the actions. [Sta+18, pp. 25-26]

2.2 Security Concepts

The security properties stated in subsection 2.1.1 Security Properties Triad and in subsection 2.1.3 Further Security Properties require to consider different security concepts. In the following section, widely-used security concepts are described.

2.2.1 Cryptography

Modern cryptography consists of two major categories: asymmetric cryptography and symmetric cryptography. Asymmetric cryptography provides encryption and digital signatures. Symmetric cryptography allows encryption and message authentication. Encryption is used to prevent unauthorized parties from reading confidential information. Digital signatures and message authentication are used to verify the integrity of data and the authenticity of the sending party. [Sta+18, pp. 52-85]

Asymmetric cryptography bases on key pairs of two related keys, a private key and a public key. The private key has to remain secret and the public key can be published. Related private and public keys are linked by certain mathematical properties. These mathematical properties restrict the execution of certain cryptographical operations

to a holder, and only a holder, of a public or private key. For security reasons, the mathematical properties that link two keys rely on an underlying trapdoor function. A trapdoor function is a function that can be easily performed one-way, but is very difficult to reverse given a certain secret is unknown. Modern asymmetric cryptography commonly uses the discrete logarithm problem and the integer factorization problem to construct trapdoor functions. [Sta+18, pp. 67-72]

Symmetric cryptography is based on a single shared key. Entities that use symmetric encryption are required to securely distribute the shared key between the participating parties. In case the key is disclosed to an untrusted third party, any cryptographic operations performed in the past, present, or future with this key cannot be considered secure anymore. Algorithms in symmetric cryptography perform various transformations and substitutions on the data that is to be encrypted or authenticated. [Sta+18, pp. 53-67]

2.2.2 Secure Hash Functions

Secure hash functions support modern cryptography. Secure hash functions are non-reversible functions, that allow to produce a *fingerprint* of data that uniquely identifies the data [Sta+18, pp. 62-67]. To be secure, a hash function H must have the following properties [Sta+18, pp. 62-67]:

First pre-image resistance – In reasonable time, it is not possible to calculate a pre-image x' for a known y, where $H(x') = y$. This must hold for all possible y.

Second pre-image resistance – In reasonable time, it is not possible to calculate a pre-image $x'(x' \neq x)$ that fulfills $H(x) = H(x')$ for a given pre-image x.

Collision resistance – In reasonable time, it is not possible to find two different values x and x' that result in the same output, i.e., $H(x) = H(x')$. Collision resistance implies second pre-image resistance.

2.2.3 Asymmetric Encryption

Asymmetric encryption allows a holder of a private key, and only a holder, to decrypt data that has been encrypted by a holder, and only a holder, of the corresponding public key. [Sta+18, pp. 67-72]

Figure 2 displays asymmetric encryption on the example of two participating parties Bob and Alice. In this example, Bob encrypts arbitrary plaintext X with an encryption function E using Alice's public key PU_a. He has chosen Alice's public key from his public key ring. A key ring is essentially a database of public keys. After encryption, Bob sends the ciphertext Y to Alice. Alice can decrypt the ciphertext Y with the decryption function D using her private key PR_a to obtain the plaintext X. [Sta+18, pp. 67-72]

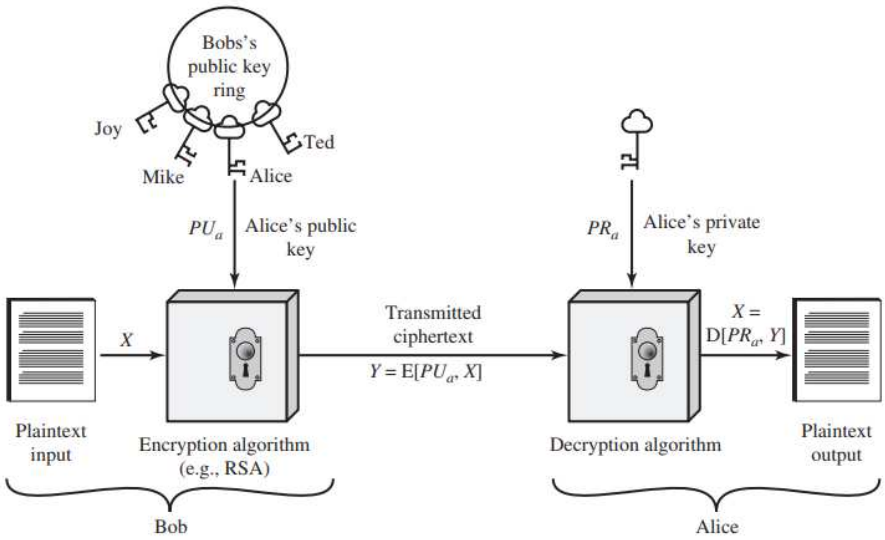


Figure 2: Asymmetric Encryption in an Example with Bob and Alice [Sta+18, p. 69]

2.2.4 Digital Signatures

Digital signatures allow a holder of a private key, and only a holder, to sign data with their digital signature. A holder of the corresponding public key, and only a holder, can verify that the signed data has not been altered and comes in fact from the holder of the private key. Signature creation and verification involve hashes calculated with secure hash functions. This allows the signing of arbitrarily long messages and prevents attacks on the digital signature. [Sta+18, pp. 72-77]

Digital signatures function similarly to asymmetric encryption. Assume Bob wants to send Alice a message and Alice wants to verify that the message comes in fact from Bob. For that, Bob signs arbitrary plaintext X with a signature function S using his private key PR_b. This produces a signature S_x. Bob then sends the concatenation $Y = X|S_x$ of the plaintext X and the signature S_x to Alice. Alice selects Bob's public key PU_b from her public key ring. With Y and PU_b, Alice can verify that the plaintext X was in fact sent by Bob. [Sta+18, pp. 72-77]

2.2.5 Symmetric Encryption

Symmetric encryption allows a holder of a shared key, and only a holder, to encrypt and decrypt arbitrary data in communication with another holder of the same shared key. Symmetric encryption distinguishes two major types of algorithms: block cipher algorithms and stream cipher algorithms. While the former are designed to encrypt data in fixed-size blocks, the latter are designed to encrypt data continuously. [Sta+18, pp. 53-59]

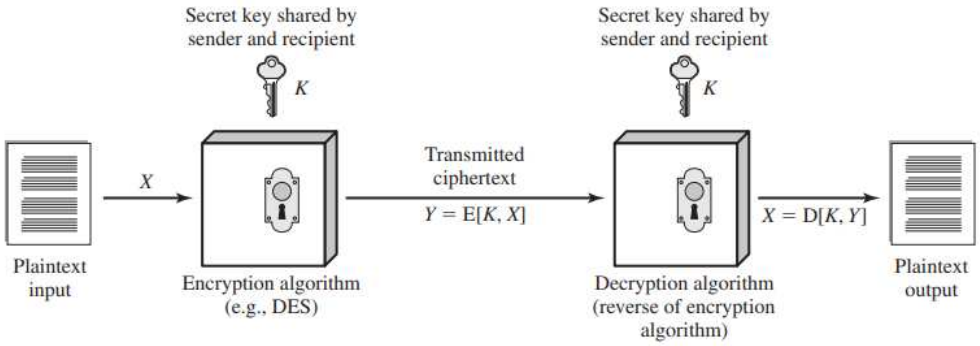


Figure 3: Symmetric Encryption Process [Sta+18, p. 54]

Popular modern symmetric cryptographic algorithms are the block cipher algorithm Advanced Encryption Standard (AES) by Daemen and Rijmen [DR99] and the stream cipher algorithm ChaCha20 by Bernstein [Ber08].

The concept of symmetric encryption is displayed in Figure 3. A plaintext X is encrypted with a shared key K using an encryption function E by a holder of K. This encryption functions outputs a ciphertext Y. Another holder of the shared key K can decrypt Y with the decryption function D to obtain the plaintext X. [Sta+18, pp. 53-59]

2.2.6 Message Authentication

Message authentication allows a holder of a shared key, and only a holder, to generate a Message Authentication Code (MAC) over an arbitrary message using their shared key. Another holder, and only a holder, of the same shared key that wants to verify the MAC, can generate a MAC over the received message themselves. If the data has not been modified and the shared keys are the same, the generated authentication code matches the initial authentication code. In that case, a verifier can be sure that the data has not been modified by a third-party. [Sta+18, pp. 59-64]

The process of MAC generation and MAC verification is depicted in Figure 4. An arbitrary sender calculates a MAC over an arbitrary message X using a MAC algorithm and a shared key K. The sender sends the concatenation $Y = X|MAC$ of the message X and the MAC to a recipient with the same shared key K. The recipient calculates a MAC over the message X using the same MAC algorithm as the sender. Then, the recipient compares the MAC they calculated with the MAC that they has received from the sender. [Sta+18, pp. 59-64]

2.2.7 Authenticated Encryption

Providing data confidentiality, integrity, and authenticity of data is a non-trivial problem. Authenticated encryption is a field in cryptography that discusses this problem and its

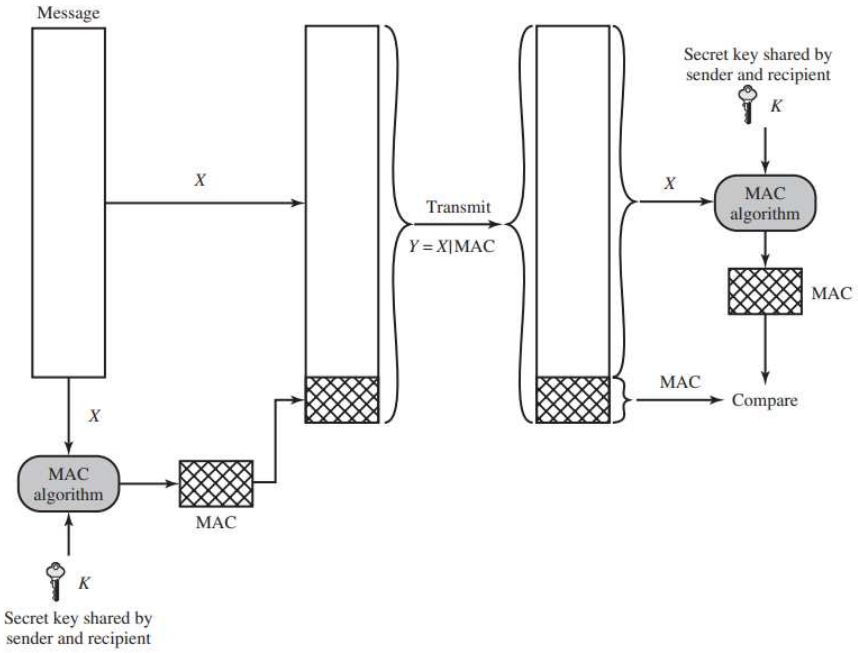


Figure 4: MAC Generation and Verification Process [Sta+18, p. 61]

solutions. Insecure solutions to this problem can lead to serious attacks. In potential solutions, a supposedly secure data blob is composed of plaintext data. [BN00]

Bellare and Namprempre [BN00] analyze authenticated encryption in the context of symmetric cryptography, looking at three major composition methods: encrypt-and-MAC plaintext, MAC-then-encrypt, encrypt-then-MAC.

Under the assumption that the given encryption scheme is IND-CPA and the used MAC is strongly unforgeable, encrypt-then-mac is IND-CPA, IND-CCA, NM-CPA, and NM-CCA. Under the same assumptions, encrypt-and-MAC plaintext and MAC-then-encrypt lack IND-CPA, IND-CCA, NM-CPA and NM-CCA, and IND-CCA, NM-CPA and NM-CCA respectively. [BN00]

2.2.8 Trusted Computing and Establishing Trust

To explain trusted computing, the definition of trust must be clarified. In current research, there are multiple definitions of trust. This thesis follows the widely-used definition formulated by Gambetta [Gam00]:

> Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such

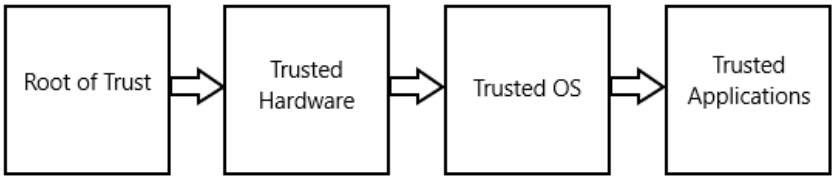


Figure 5: Trust Chain in Trusted Computer Systems [Hua+06]

> action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.

Trust can be obtained through two major ways: directly and indirectly. If a party X has interacted with a party Y in the past, then the level of trust in Y can be measured by reviewing the past behavior of Y. This type of trust is called direct trust. If the party X has not interacted with the party Y in the past, the party X may ask another party Z for its direct trust value with party Y. This type of trust is called indirect trust. In some cases, there are many levels of indirection. The resulting chain is called a trust chain. [Hua+06]

Trust chains are based on a root of trust or trust anchor. In trusted computer systems, for example, the chain evolves from the root of trust, over the trusted hardware platform, to the trusted operating system, and finally to the trusted applications. Every element in the chain checks the integrity of the next element before executing it and passing trust to it. This concept is displayed in Figure 5. [Hua+06]

In cryptography, there are three major ways to establish trust in public use [Sta+18, pp. 80, 707–716]: X.509 by Cooper et al. [Coo+08], the Pretty Good Privacy (PGP) by Garfinkel [Gar95], and Kerberos by Miller and Neuman [Mil+87] based on the work of Needham and Schroeder [NS78].

In X.509 and Kerberos, a party is either trusted or untrusted [Sta+18, pp. 707-716], i.e., there are no gradual levels of trust. In the PGP, there are gradual trust levels [Gar95]. These levels allow participating parties a more nuanced trust decision [Gar95].

X.509 describes a hierarchical Public Key Infrastructure (PKI) model. In X.509, the participating parties do not trust each other directly. Instead, they all directly trust common third-parties of the PKI: Certificate Authorities. As a result, participating parties indirectly trust each other. If a party X can prove that a Certificate Authority (CA) trusts them, another party Y can be sure that the party X is trustworthy. [Sta+18, pp. 713-716]

Much like X.509, Kerberos is an authentication system that relies on a trusted third-party. In Kerberos, the trusted third-party is called Key Distribution Center (KDC). If a party X can prove that the KDC trusts them directly, another party Y can be sure that the party X is trustworthy. [KL14, pp. 361-363]

Unlike in X.509 and Kerberos, in PGP there are no central trusted parties. Instead, participating parties are expected to establish trust relations with each other. In PGP, a party X can sign the public key of another party Y and assign the signature a trust level. The public key of party Y can have multiple signatures. The trust of these signatures accumulates. This technique allows a party Z to decide whether the accumulated trust of party Y is sufficient for the action party Y wants to perform on the party Z's system. [Gar95]

2.2.9 Audit Trail

An audit trail is one or more logs that record important events in an IT system. In IT security, audit trails provide means to link security-relevant events to parties of the IT system. As such they are themselves security-relevant. [Lan01]

2.2.10 Denial-of-Service

NIST SP 800-27 Revision A [Sto+04] defines Denial-of-Service (DoS) as

> The prevention of authorized access to resources or the delaying of time-critical operations.

There are several categories of resources that could be attacked [Sta+18, p. 248]:

- Network bandwidth [Sta+18, p. 248]
- System resources [Sta+18, p. 248]
- Application resources [Sta+18, p. 248]

Networks have limited bandwidth. As a result, when the bandwidth limit is hit packets have to be discarded or packet delivery has to be delayed. [Sta+18, pp. 241-242]

Systems have limited resources to process packets. When these resources are exhausted, packets have to be discarded or packet processing has to be delayed. Systems are also vulnerable to bugs in their network handling software. Triggering a bug in a system's network handling software may cause it to crash. This means the system can no longer communicate over the network until this software is reloaded. For that, typically a reboot is required. [Sta+18, pp. 248-250]

Attacks on application resources typically involve several valid requests. Each of these requests consumes significant resources. As a result, requests have to be discarded or request processing has to be delayed. This impairs the ability of the application to process legitimate requests from other users. [Sta+18, pp. 248-250]

Notably, the categories listed by Stallings et al. [Sta+18, p. 248] do not include routing attacks, such as black hole attacks. Routing attacks often do not target a network's bandwidth but the network's routing mechanism (e.g., link-withholding attacks, link-spoofing attacks, or colluding misrelay attacks, as discussed in section 5.3 Attacks on the Network Layer of Vehicular Ad Hoc Networks or black hole attacks, as discussed in chapter 6 Black Hole Attacks in Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks). For the purpose of this thesis the category *network bandwidth* is extended to *network resources* to include routing attacks.

DoS attacks can be performed through a single packet (e.g., with a DNS amplification attack), a small number of packets (e.g., with the Slow Loris attack), or a large number of packets (e.g., with a Distributed DoS (DDoS)). [Sta+18, pp. 246-270]

Various steps can be taken against DoS attacks. These steps limit the likelihood and impact of DoS attacks. It is important to note that DoS attacks cannot be fully prevented. [Sta+18, pp. 259-264]

2.3 Measures to Achieve Security

The security properties stated in subsection 2.1.1 Security Properties Triad and in subsection 2.1.3 Further Security Properties can be achieved through different measures supported by security concepts described in section 2.2 Security Concepts. In the following subsections, some widely-used measures to achieve these security properties are described.

2.3.1 Data Confidentiality, Integrity, and Authenticity

Arguably, measures to achieve data confidentiality, integrity, and authenticity are strongly interrelated. The following subsection describes how data confidentiality, integrity, and authenticity can be achieved.

Data confidentiality of data in transit or at rest can be achieved through a combination of cryptography, authorization, and authentication, as discussed in the following.

Both symmetric and asymmetric cryptography can provide data confidentiality [Sta+18, pp. 52-84]. Depending on the underlying IT system's requirements, symmetric and/or asymmetric cryptography should be used for optimal results [KL14]. Common requirements for cryptography in IT systems are good performance and secure key distribution [KL14].

As described by Lin and Lu [LL15, p. 14] and by Katz and Lindell [KL14, p. 389], many algorithms in symmetric cryptography have significantly better performance than those in asymmetric cryptography.

In terms of secure key distribution, asymmetric cryptography has a significant advantage over symmetric cryptography. In asymmetric cryptography, public keys are intended to be shared. As a result, in most schemes, the public key can be shared over an insecure

channel without a decrease in security. Contrary to that, in symmetric cryptography, keys must be shared over a secure channel. [KL14, pp. 359-360]

To utilize the advantages of both types of cryptography, symmetric and asymmetric cryptography can be used in combination with so-called key-exchange protocols. [LL15, p. 14]

In key-exchange protocols, a secure channel is created through asymmetric cryptography. Then a symmetric key is shared over the secure channel. The symmetric key is used for further performant cryptographic operations. [CK01]

Authorization is the granting of privileges to a party [Sta+18, pp. 127-131] (e.g., a party X is allowed to access a directory on a server). Authorization can be achieved through Role-Based Access Control (RBAC) [Sta+18, pp. 142-148]. In RBAC users are assigned a role that holds specific privileges. The privileges of the role of a user are checked before the user can access a resource [Sta+18, pp. 142-148]. Authentication is the process to ascertain that a thing is what it claims to be [LL15, p. 8], i.e., the process of certifying authenticity. Achieving authenticity is discussed later in this subsection.

Unauthorized modification of data in transit or at rest violates the integrity property [Sta+18, p. 25]. Unauthorized modification of data can be prevented by employing secure hash functions combined with digital signatures or MACs and subsequently verifying hash values and digital signatures or MACs [Sta+18, pp. 59-67, 72–77]. Encryption alone is not sufficient to protect against unauthorized modification, as non-integrity protected ciphertext is prone to manipulation [KL14, p. 108]. A well-known example of an attack exploiting non-integrity protected ciphertext is an attack by Borisov et al. [Bor+01] on the Wired Equivalent Privacy (WEP) protocol. This attack allowed arbitrary message modifications and enabled a break of the data confidentiality supposedly provided by the stream cipher Ron's Code 4 (RC4) [Bor+01]. In a symmetric setting, the usage of authenticated encryption can prevent unauthorized modification of data [KL14, pp. 131-142].

Unauthorized modification of systems violates the integrity property [Sta+18, p. 25]. Such modification of systems can be avoided by employing trusted computing throughout the used IT systems [Sta+12, pp. 465-469].

Correctness of content cannot be fully enforced by formal or algorithmic means, but correctness of content could be checked with semantic constraints. [Bis09, p. 41]

Authenticity can be ensured through digital signatures [KL14, p. 439] or MACs [Sta+18, pp. 60-61]. As discussed in subsection 2.2.4 Digital Signatures, digital signatures allow to verify that an alleged sender of a message has in fact sent the signed message, i.e., digital signatures allow to verify that the message is authentic [KL14, p. 439]. As discussed in subsection 2.2.6 Message Authentication, MACs allow to verify that an alleged sender has in fact sent the message protected by the MAC, i.e., MACs allow to verify that the message is authentic [Sta+18, pp. 60-61]. Under the assumption that only a recipient of

a message and the sender of that message know the secret key of a MAC, MACs provide authenticity [Sta+18, pp. 60-61].

In a communication setting with symmetric cryptography, the usage of authenticated encryption is best practice [KL14, p. 131]. Authenticated encryption can provide communication with data confidentiality, integrity, and authenticity [Sta+18, p. 666].

2.3.2 Availability

The loss of availability is defined as the inability to access information or resources of an IT system. Such a loss of availability can either occur inadvertently or maliciously through a DoS attack. The more critical an IT system, the higher the availability requirements. [Sta+18, pp. 25-28]

Robustness against DoS attacks can be achieved by employing defenses against DoS attacks. Defenses against DoS attacks can be broadly divided into four categories, as described by Peng et al. [Pen+07]. Stallings et al. [Sta+18, pp. 265-269] partly bases on the work of Peng et al. and extends it. The four categories of defenses against DoS attacks are [Sta+18, pp. 265-269]:

(1) Attack prevention [Sta+18, pp. 265-269]

(2) Attack detection [Sta+18, pp. 265-269]

(3) Attack source identification [Sta+18, pp. 265-269]

(4) Attack reaction [Sta+18, pp. 265-269]

Attack prevention aims to stop attacks before they cause damage [Sta+18, pp. 265-269]. In attack prevention, it is assumed that the source address of attack traffic is spoofed and that the number of attacks will decrease if every source is accountable [Pen+07]. Attacks using spoofed source addresses continue to occur frequently [Sta+18, p. 252]. However, there are DoS attacks without spoofed source addresses (e.g., DDoS attacks [Sta+18, pp. 256-258]). As a result, relying solely on attack prevention schemes is not sufficient to stop DoS attacks [Pen+07].

An example of a prevention mechanism is ingress/egress filtering. In ingress/egress filtering, traffic coming in a local network (ingress) and traffic leaving a local network (egress) is filtered to only come from allowed sources and go to allowed destinations. [Sta+18, pp. 266-267]

In addition to other prevention schemes, if an organization is dependent on network services, servers could be replicated or mirrored over multiple sites with multiple network connections to prevent DoS attacks. [Sta+18, pp. 265-269]

Attack detection is the next step of DoS defense, after attack prevention [Sta+18, p. 266]. Ideally, attacks should be detected before a user of the IT system notices a

loss of availability [Sta+18, pp. 269-270]. Attacks could be detected beforehand by automatic network monitoring and intrusion detection systems that monitor abnormal traffic [Sta+18, pp. 265-269]. For such a measure to be successful, an organization should know its normal traffic pattern [Sta+18, pp. 265-269].

An example of a detection mechanism is MUlti-Level Tree for Online Packet Statistics (MULTOPS) by Gil and Poletto [GP01]. MULTOPS assumes that packet rates of uplinks and downlinks between two hosts are proportional in an honest scenario. A strong disproportion indicates a DoS attack. [Pen+07]

Ideally, after attack detection, the source of the attack traffic should be identified [Sta+18, p. 266]. However, it is not always easy to track attack traffic to its source. Employing source traceability can solve this issue [Sta+18, pp. 269-270].

An example of a source identification mechanism is hash-based Internet Protocol (IP) traceback by Soeren et al. [Sno+01]. In hash-based IP traceback, routers keep records of packets passing through the router. These records are hash digests of the packets. When a traceback is required, a host sends a traceback query for a specific packet to its router. This router, in turn, passes the query to its neighboring routers. The traceback process is repeated until the packet origin is located. [Pen+07]

The last step of achieving robustness against DoS attacks is attack reaction [Sta+18, p. 266]. In the following of a DoS attack, the attack should be analyzed and measures should be drawn from this analysis to improve the future handling of attacks [Sta+18, pp. 269-270]. Additionally, to minimize the damage of future attacks, an attack reaction scheme can be employed [Pen+07].

An example of a reaction scheme is a congestion signature-based scheme by Mahajan et al. [Mah+02]. In this scheme, routers learn a congestion signature that can differentiate legitimate traffic from malicious traffic based on the volume of the traffic to the target coming from different links. Based on the congestion signature, routers filter malicious traffic. [Pen+07]

2.3.3 Accountability

Accountability allows authorized third-parties to hold parties of an IT system accountable for their actions [Sta+18, p. 26]. Accountability requires authenticity as a prerequisite [Sta+18, p. 86] and further needs actions to be traceable to its origin [Sta+18, p. 14]. For example, when using digital signatures with PKI, the origin of an action can be obtained from the certificate that was used for the digital signature. More generically in an unspecified IT system, traceability of origin can be achieved through audit trails [Sta+18, p. 132]. Audit trails can be useful for system administration and maintenance [Sta+18, p. 584]. In IT Security, one major problem of audit trails is finding security-relevant events in the mass of log entries [Sta+18, pp. 600-603].

As audit trails are themselves security-relevant, they are prone to attacks. An attacker, who has attacked an IT system belonging to an audit trail, would often wish to cover

his tracks to prevent prosecution. As a result, audit trails need to be made resistant to attacks. For example, logs can be written to a write-once device to prevent retroactive destruction of the audit trail. [Lan01]

SELinux, designed by Loscocco and Smalley [LS01b], is an example of an IT system that enables an audit trail. SELinux is a Linux security module [Sma+01]. It has been designed to meet high-security requirements. Broadly speaking, the security concept of SELinux bases on subjects (processes), objects (e.g., files, sockets, or network interfaces), and a security policy [LS01b]. The security policy allows enforcing fine-grained mandatory access control on subjects and objects [LS01b]. SELinux allows configuring audit rules for access events [Ver17, pp. 42-64]. Audit rules enable administrators to configure logging *access granted* events and *access denied* events to a log directory [Ver17, p. 49].

2.3.4 Privacy

Depending on the privacy requirements of the underlying IT system, the IT system should be designed in a way that the IT system preserves none to all of the properties of privacy. Privacy preservation can be achieved through various schemes, which are described later in this subsection.

As attackers presumably do not forget any actions, the privacy properties anonymity, unlinkability, and unobservability need to be preserved preemptively [PH10].

Anonymity can be achieved by basing authorization and access control on non-personal information of a party [Sta+18, pp. 614-655]. In many cases, however, some personal information is required for the functionality of the IT system. In such cases, even when very specific identifiers, such as the name or exact address, are not present in the IT system, parties could be deanonymized. Examples for such deanonymization attacks are homogeneity attacks or a background knowledge attacks [Mac+07]. Both are discussed by Machanavajjhala et al. [Mac+07]. Generally, per-action decreases of anonymity should be kept low [PH10].

Pseudonymity can be achieved by providing parties with aliases and only disclosing the aliases to other parties in the IT system, but holding a link with personal information to that alias. As a result, parties other than the administrators cannot identify other parties, but administrators can still identify parties to hold them accountable. [Sta+18, pp. 614-615]

Unlinkability can be achieved by keeping the probability that observed actions have been performed by a party sufficiently close to $1/number\_of\_parties$. It is desirable to keep incremental decreases in unlinkability as low as possible. [PH10]

Unobservability can be achieved by keeping unobservable if a party has used an IT system. The state of complete unobservability is called perfect unobservability. Incremental decreases of unobservability should be kept as low as possible. [PH10]

The Dining Cryptographers Network (DC-net) by Chaum [Cha85; Cha88], the Mix-net by Chaum [Cha81], the improved DC-net (DC^+-net) by Waidner [Wai89] and private

information retrieval by Cooper and Birman [CB95] are mechanisms to achieve certain forms of anonymity. If dummy traffic is added, all of them provide unobservability. [PH10]

CHAPTER 3

Fundamentals of Intelligent Transport Systems

In this chapter, the fundamentals of Intelligent Transport Systems (ITS) are explained. These fundamentals include a general overview of ITS and a description of ITS and VANETs. This description includes a detailed discussion of the International Organization for Standardization/Open System Interconnection (ISO/OSI) of ITS/VANETs.

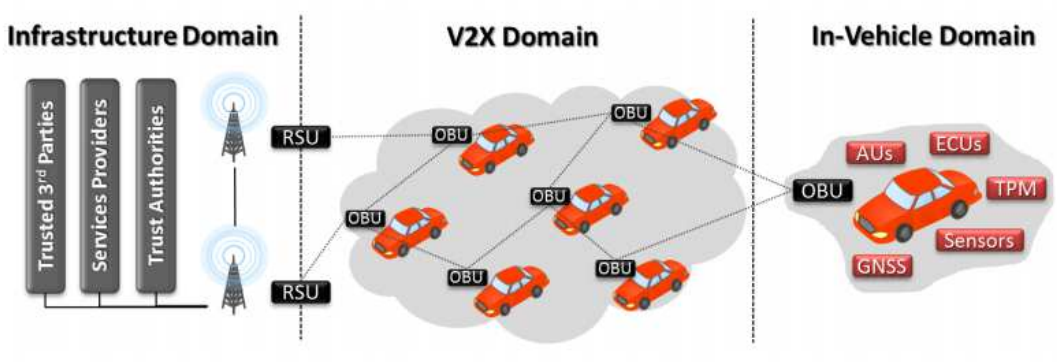
3.1 Overview

ITS are systems that integrate information exchange technologies and communication technologies in transport infrastructure. [LC16]

ITS have emerged from vehicles in the 1970s. Initially, vehicles have been equipped with sensors due to stringent emission regulations. The number of sensors has since increased significantly because of an increased demand for efficiency and performance. With the increase of sensors, their functionality diversified from emission tracking to numerous other use cases. Up until recently, sensor data has mostly been exchanged within a vehicle, while there is still a lot of untapped potential in the exchange of data between vehicles. Potential improvements include major advancements in road safety, reduced operating costs, and increased efficiency, comfort, and convenience. [Sie+17]

The interconnection of vehicles is likely to steadily increase to achieve these potential improvements [Ham+15]. ITS are upcoming solutions to enable an interconnection of vehicles on a large scale [Ham+15]. In the context of ITS, vehicles are often referred to as Smart Vehicles, since they appear to solve problems intelligently [Men+18, pp. 24-25].

ITS architecture, as displayed in Figure 6, is a high-level architecture consisting of three main communication domains [Ham+15]:



V2X=Vehicle-To-Anything, **AU**=Application Unit, **ECU**=Electronic Control Unit, **TPM**=Trusted Platform Module, **GNSS**=Global Navigation Satellite System, **RSU**=Road-Side Unit, **OBU**=On-Board Unit

Figure 6: ITS Archictecture [Ham+15]

- the In-Vehicle Domain, in which a Smart Vehicle internally exchanges data through various On-Board Units (OBUs). [Ham+15]
- the Vehicle-to-Anything (V2X) Domain, in which Smart Vehicles communicate with other Smart Vehicles and various RSUs. [Ham+15]
- the Infrastructure Domain, which provides various services for Smart Vehicles via RSUs. [Ham+15]

As common VANETs standard sets, such as the European Telecommunications Standards Institute (ETSI) Cooperative Intelligent Transport Systems (C-ITS) and the Wireless Access in Vehicular Environments (WAVE), reside in the V2X Domain, this thesis focuses exclusively on the V2X domain in the following. [Fes15]

Communication in the V2X domain (aka V2X communication) occurs wirelessly in potentially large VANETs [Men+18, pp. 27-29, 53, 79]. In such a setup, information can severely affect lives, making attacks on the system or its participants potentially fatal [LL15, p. 22].

As a result, the common VANET standard sets are designed with security measures that prevent attacks (e.g., ETSI [Ins13b] or WAVE [Gro16]).

3.2 Terminology in Intelligent Transport Systems Research

As an umbrella term ITS consists of various technologies of which the most relevant are: Smart/Connected Vehicles, the V2X Domain, and VANETs. These terms are described in the following subsections.

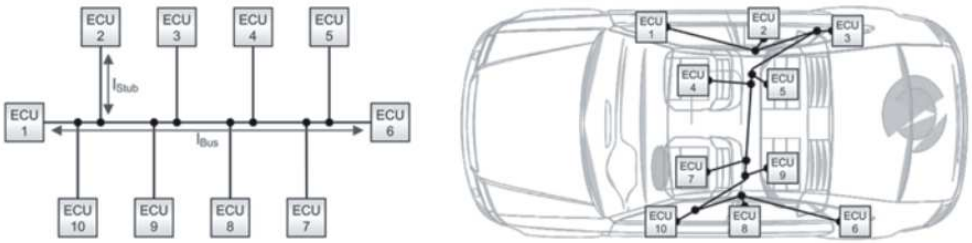


Figure 7: Linear Bus Topology for the In-Vehicular Exchange of Sensor Data [Law+13, p. 54]

3.2.1 Differences and Characteristics of Modern Vehicles and Smart Vehicles

Nowadays, vehicles are equipped with numerous sensors to provide various functionality, such as the preemptive tension of seat-belts right before a collision or the prediction of common destinations. The generated sensor data is currently mostly used for in-vehicle functionality and therefore exchanged internally. [Sie+17]

There exist various bus technologies allowing such an internal exchange of sensor data. Senders and receivers of sensor data are so-called Electronic Control Units (ECUs). Among well-known in-vehicle buses are the Controller Area Network (CAN) bus by the Robert Bosch GmbH [Gmb91], the Local Interconnect Network (LIN) bus by the LIN Consortium [Con10], and FlexRay by the FlexRay Consortium [Con05]. [Men+18, pp. 24-27]

A possible bus topology is displayed in Figure 7.

Smart Vehicles are also referred to as Connected Vehicles in current research (e.g. Meneguette et al. [Men+18] or Lu et al. [Lu+14]).

Just as modern vehicles, Smart Vehicles are equipped with numerous sensors, multiple networking interfaces, and a central processing unit. Unlike modern vehicles, Smart Vehicles can communicate with other Smart Vehicles or RSUs via wireless communication devices. The feasibility of such communication is heavily dependent on the underlying network. [Men+18, p. 15]

3.2.2 Vehicle-To-Anything Domain

As displayed in Figure 6, the V2X Domain mainly comprises of Smart Vehicles and various RSUs that are located along the roads [Ham+15]. In the V2X Domain, information is exchanged via V2X communication and occurs between Smart Vehicles and RSUs [Ham+15]. V2X communication can be divided into three major categories: Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure/Infrastructure-to-Vehicle (V2I/I2V) communication, and a hybrid of V2V communication and V2I/I2V communication [LL15, p. 12].

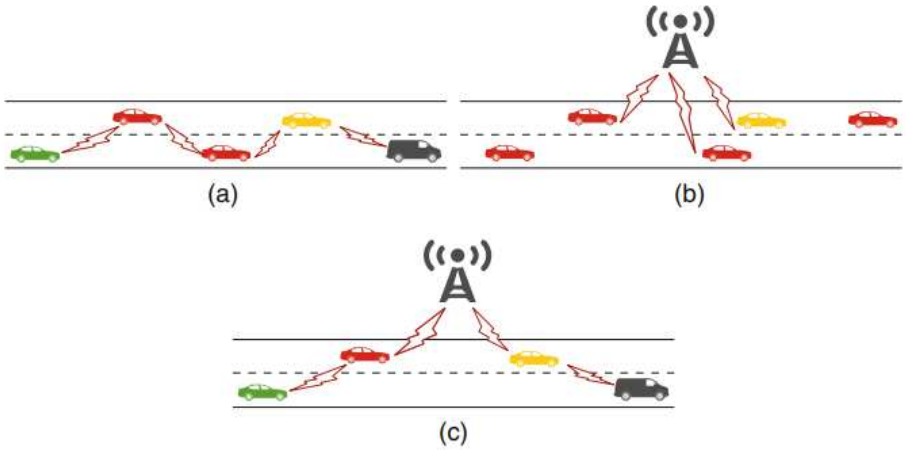


Figure 8: V2X Communication Types: (a) Vehicle-To-Vehicle Communication; (b) Vehicle-To-Infrastructure Communication; (c) Hybrid Communication; [Men+18, p. 27]

The concept of V2V communication, V2I/I2V communication, and hybrid communication is displayed in Figure 8. V2X communication either happens through short-range wireless communication or other established wireless technologies, such as WiMax or the 5th Generation (5G) of cellular networks [Men+18, p. 27].

3.2.3 Vehicular Ad Hoc Networks

Networks hosting V2X communication are known as VANETs [Men+18, pp. 27-28]. VANETs have specific characteristics, but as a subgroup of Mobile Ad Hoc Networks (MANETs), VANETs also inherit many characteristics and properties from MANETs (e.g., self-organization, low bandwidth, or wireless short-range communication) [Men+18, pp. 28-29]. The relation between MANETs and VANETs and current research in MANETs is described in more detail in section 9.4 Mobile Ad Hoc Networks. Meneguette et al. [Men+18, pp. 28-29] list the following characteristics of VANETs:

- Self-Organization – VANETs are self-organized networks. This characteristic is inherited from MANETs. [Men+18, pp. 28-29]
- High Mobility – Nodes in VANETs are highly mobile compared to other wireless networks. However, they are limited to infrastructure, such as roads or garages. [Men+18, pp. 28-29]
- Fast Transmission Speed – Since nodes can reach high speeds, the time of contact with a VANET might only be a few seconds. As a result, transmission speeds have to be fast. [Men+18, pp. 28-29]
- Short-Lived Topology – The high mobility of nodes leads to fast changes in topology. Such fast changes might be challenging to manage. [Men+18, pp. 28-29]

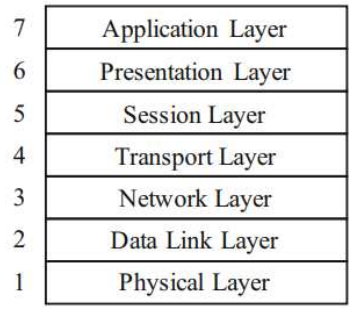


Figure 9: ISO/OSI Reference Model [Gün+17, pp.14-15]

- Ample Energy Constraints – Unlike in other manifestations of MANETs (e.g., internet-based Mobile Ad hoc Network (iMANET [RD13])), nodes in VANETs can rely on relatively ample energy constraints. Therefore, they can be equipped with significant computational power. [Men+18, pp. 28-29]

- Flexible Communication – Nodes in a VANET can contain hardware that supports multiple wireless communication technologies. Thus, nodes can reach different networks. With sophisticated communication strategies, it is possible to utilize these different networks to combat issues with connectivity and bandwidth. [Men+18, pp. 28-29]

- Network Fragmentation – Due to the high dynamism of nodes and the restricted communication radius of wireless communication, network fragmentation is common in VANETs. [Men+18, pp. 28-29]

The well-known ISO/OSI protocol stack model by Day and Zimmermann [DZ83] is commonly used for describing and discussing computer networks. The standard protocol stack model consists of the layers: physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. These layers are displayed in Figure 9.

In computer network literature, the ISO/OSI protocol stack model is often modified, because the presentation layer and the session layer are not implemented independently, particularly in the Internet [Gün+17, pp.14-15]. For the usage in wireless multi-hop networks, such as VANETs, Güneš et al. [Gün+17, pp.14-15] remove the data link layer, the presentation layer, and the session layer. Similarly this thesis removes the presentation layer and the session layer but keeps the data link layer. In common VANET standard sets the data link layer is used but neither the presentation layer nor the session layer are present (e.g., ETSI [Ins10b] or WAVE [Li10]). The network stack model used for the description of VANETs in this thesis is displayed in Figure 10.

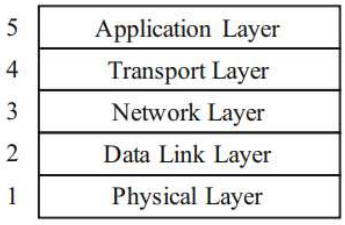


Figure 10: Network Stack Model Modified for VANETs (cf. [Gün+17, pp.14-15])

Physical Layer

Dedicated Short-Range Communication (DSRC) is used at the physical layer of common VANETs (e.g., ETSI C-ITS or WAVE) [Cun+16]. DSRC is a generic name for short-range, point-to-point communication in the worldwide reserved 5.9 GHz frequency band [Sin+14]. DSRC supports node speeds of up to 200km/h, has a transmission range of up to 1000m and data rates of up to 27Mbps [Cun+16].

Common VANET standard sets make use of a dedicated V2X communication frequency band within the 5.9 GHz frequency band (e.g., ETSI [Ins10a] or WAVE [Men+18, pp. 29-32]). The dedicated V2X communication frequency band is further divided into channels, some of which are reserved for road safety applications and some of which are reserved for general-purpose ITS services [Cun+16].

Data Link Layer

Common VANET standard sets subdivide the data link layer into Media Access Control (MAC) layer and Logical Link Control (LLC) layer (e.g., ETSI [Ins10b] or WAVE [Fer+18]).

The MAC layer specifies how nodes access the underlying channel [Gil+15]. Common VANET standard sets further subdivide the MAC layer in the lower and upper MAC layer, also known as MAC extension layer (e.g., ETSI C-ITS or WAVE) [Fer+18]. The lower MAC layer defines the node access mechanism [Fer+18].

Lower Mac Layer

Gilliani et al. [Gil+15] list three major types of lower MAC layer protocols:

- Contention-free protocols: In contention-free protocols, a central party is often responsible for pre-allocating access to a channel. There is no competition for channel access and the protocol may guarantee Quality of Service (QoS). Therefore, such protocols can be suitable for road safety applications in VANETs. [Gil+15]

  Suitable candidates for contention-free protocols in VANETs might be Time Division Multiple Access (TDMA), Space Division Multiple Access (SDMA) and Code

Division Multiple Access (CDMA). In TDMA time slots are used to regulate channel access. In SDMA, channel access is granted based on the location of a node. [Oma+12]

In CDMA, simultaneous multi-user channel access is made possible by assigning signature waveforms to each user. Knowledge of the respective waveform allows demodulating the data streams of the respective users. [LV89]

- Contention-based protocols: Contention-based protocols are protocols where nodes compete for channel access. Whichever node wins the competition can use the channel for the negotiated time. Real-time delivery of road safety messages may not be guaranteed in such protocols. Therefore, some form of congestion control may be required for road safety applications in VANETs. [Gil+15]

  Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) by Gallager [Gal85] is a well-known contention-based protocol. In CSMA/CA a node listens to the network before transmitting a frame. If the channel is idle, the node performs a predefined collision avoidance procedure. If the channel is busy, the node waits until the end of the ongoing transmission and then competes for channel access through a predefined back-off procedure. [WK05]

- Hybrid protocols: Hybrid protocols are mixtures of different contention-free and/or contention-based protocols. [Gil+15]

  Suitable candidates of hybrid protocols for VANETs are discussed by Nguyen et al. [Ngu+16] and Dang et al. [Dan+14].

MAC Extension Layer

In common VANET standard sets, the MAC extension layer is used to enable multi-channel operations and enhance channel access (e.g., ETSI C-ITS or WAVE). Such enhancements include prioritization and scheduling of messages. [Fer+18]

Logical Link Control Layer

Common VANET standard sets use the LLC layer for the selection of the network protocol and potentially also for the selection of the transport protocol (e.g., ETSI [Ins19] or WAVE [Men+18, p. 31]).

Network Layer

Network protocols extend the connectivity from single-hop to multi-hop connectivity in a VANET. The connectivity between nodes relies heavily on the cooperative reaction of the nodes of the network. [Pat11, p. 202]

The network layer is responsible for addressing, routing and transmitting data between nodes. [Men+18, pp. 32-34]

Addressing

Addressing takes care of properly addressing network nodes. In VANETs there are several possible addressing techniques. The most common strategies are fixed addressing and geographic addressing. In fixed addressing each node gets assigned a fixed address by a mechanism when it enters the network. In geographic addressing, each node receives a dynamic address based on its geographic location. This address changes as the node's geographic location changes. Regardless of the addressing strategy an address must be unique to one single node. [Men+18, pp. 32-34]

Routing

Routing is responsible for finding the best communication paths, so that data is delivered in the shortest possible time. For such functionality, delivery must be independent of the communication range of a single wireless hop. Therefore, packets must be forwarded in an arbitrary amount of single hops, also referred to as multi-hop communication. [Men+18, pp. 32-34]

VANETs support various dissemination paradigms based on multi-hop communication [Cun+16]. These paradigms are well-known from common network protocols, such as the IP version 6 (IPv6) by Deering and Hinden [DH17] and can be categorized by the number of recipients [Met02]:

- Unicast allows a source node to communicate with another specific node. [Met02]
- Anycast allows a source node to communicate with one arbitrary node in the network. [Met02]
- Multicast allows a source node to communicate with multiple nodes. These nodes share a common property or feature. [Met02]
- Broadcast communication allows a source node to communicate with all nodes in the network. This is effective for disseminating information and is often used for discovering network nodes for routing purposes. [Met02]

Numerous VANET routing protocols are discussed in current research (e.g., Ad hoc On-demand Distance Vector (AODV) routing by Perkins and Royer [PR99], Greedy Perimeter Stateless Routing (GPSR) by Karp and Kung [KK00], Greedy Traffic Aware Routing (GyTAR) by Jerbi et al. [Jer+07], or Vector-based TRAcking DEtection (V-TRADE by Sun et al. [Sun+00]) [Cun+16]. A summary of such protocols has been done by Cunha et al. [Cun+16].

Routing protocols are categorized varyingly in current research. Well-known categorizations have been done by Meneguette et al. [Men+18, pp. 84-103], by Paul et al. [Pau+12], by Singh and Agrawal [SA14], and by Kumar and Dave [KD11]. This thesis employs the categorization of Meneguette et al. [Men+18, pp. 84-103].

Ad Hoc Routing Protocols are based on network topology, i.e., the distribution of nodes in the network and information about their linkage. There are the following subclasses of Ad Hoc Routing Protocols [Men+18, pp. 85-87]:

- Proactive – In proactive protocols topology information is stored in a table. On topology changes, the information in the table is updated, consuming network bandwidth. Due to frequent topology changes in VANETs, proactive protocols may be inefficient for VANETs. [Men+18, pp. 85-87]
- Reactive – Reactive protocols do not include a routing table. Instead, a route is found on-demand. On-demand routing introduces some delay. Route discovery is facilitated through a flooding mechanism, that can introduce a substantial network overhead in VANETs. Flooding mechanisms typically cause each node to forward received messages to all its neighbors. Thereby flooding ensures the delivery of messages to all nodes in a VANET. [Men+18, pp. 85-87]
- Hybrid – Hybrid protocols are a combination of reactive and proactive protocols and aim to minimize the network delay and the network overhead of each protocol type. [Men+18, pp. 85-87]

Geographic Positioning Protocols use geographic information to find a route. Senders need information about their location and their neighbors' location. The source of this information can be city maps, traffic patterns, or the node's on-board navigation systems. Geographic Positioning Protocols are very promising for VANETs. However, they face several challenges. Among these challenges are unequal distribution of nodes, mobility restricted by road patterns, and obstacles that cause a disconnection from the network. [Men+18, pp. 87-92]

Cluster protocols create a virtual network infrastructure between nodes by clustering them. Each resulting cluster can have a cluster head, which is responsible for intra- and intercluster coordination in the network. Nodes within a cluster communicate directly, while intercluster communication is performed through cluster heads. For intercluster communication, cluster heads can facilitate other nodes as gateways. The selection of cluster heads and cluster gateways has been shown to be a great challenge in cluster protocols. Cluster protocols are especially fitting for highway environments, where nodes can naturally form long-lasting clusters. Cluster protocols may suffer from several problems in urban or rural environments, due to more frequent changes in topology. [Men+18, pp. 93-94]

Broadcast protocols have several purposes in VANETs. The most prevalent purpose is the dissemination of various ITS application information. The easiest way to broadcast information is to use flooding mechanisms. While flooding mechanisms perform well for a limited number of nodes in a network, flooding mechanisms in networks with a large number of nodes may cause significant decreases in performance. To avoid overloading the network with unnecessary messages it is therefore recommended to perform flooding

management. Flooding management aims to limit the number of unnecessary messages during flooding. [Men+18, pp. 94-97]

Multicast protocols are made to deliver messages to a group of nodes. As data in VANETs is sent wirelessly, multiple nodes can naturally receive the sent data. Multicast groups that would receive certain data are commonly managed through tree structures or meshes. [Men+18, pp. 97-101]

Geocast protocols are fundamentally multicast protocols based on geographic positions. They aim to transmit messages to all nodes within a geographic target area. Geocast protocols are mostly based on directed flooding. Directed flooding tries to limit the network overhead of undifferentiated flooding by only targeting a relevant area. Geocast protocols do not perform well in low-density environments, since the network fragmentation is high there. [Men+18, pp. 101-104]

The combination of various routing protocols and dissemination paradigms lead to the following terms in current research: GeoUnicast/Unicast in a geographic manner (e.g., the European Telecommunications Standards Insitute [Ins14d] or Meneguette et al. [Men+18, pp. 32–34]), GeoAnycast (e.g., the European Telecommunications Standards Insitute [Ins13a] or Kaiwartya and Kumar [KK15]), Geocast/Multicast in a geographic manner (e.g., Meneguette et al. [Men+18, pp. 32–34]), and GeoBroadcast (e.g., Liu et al. [Liu+15]). Due to the ambiguity of these terms, they are sometimes used inconsistently in current research. For example, Meneguette et al. [Men+18, pp. 32–34]) use Geocast for communication between a source and a group of nodes in a geographic target area, while Liu et al. [Liu+15] describe the same communication with GeoBroadcast. As a result of the inconsistent usage of these terms, this thesis employs its own definitions as displayed in Figure 11 and described as follows:

- GeoUnicast – A source node communicating with another node at a specific location.
- GeoAnycast – A source node communicating with one arbitrary node within a geographic target area.
- GeoMulticast – A source node communicating with multiple nodes that have certain features (e.g., a certain car brand) within a geographic target area.
- GeoBroadcast – A source node communicating with all nodes within a geographic target area.

Transport Layer

Traditional transport protocols, such as the Transport Control Protocol (TCP) [Pos81] and User Datagram Protocol (UDP) [Pos80], are inefficient in VANETs. [Men+18, pp. 34-35]

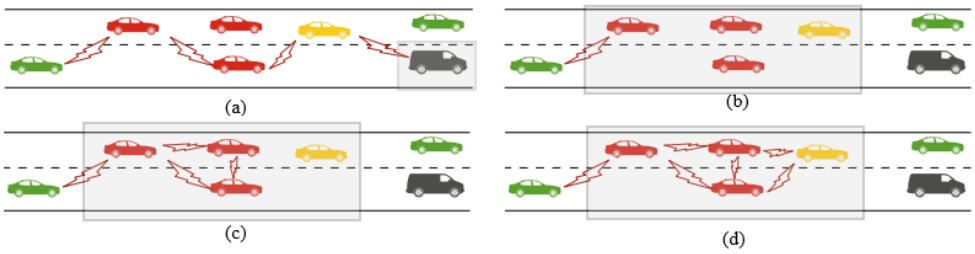


Figure 11: Common Dissemination Paradigms in VANETs: (a) GeoUnicast; (b) GeoAnycast Communication; (c) GeoMulticast Communication; (d) GeoBroadcast Communication; (cf. [Men+18, pp. 32–34])

In TCP, packet loss is treated as a sign of network congestion. However, in VANETs losses can occur for other reasons, such as channel conditions or collisions. Unaware of this, TCP reduces the size of the congestion windows and therewith decreases the throughput. TCP performance may be further diminished due to incorrect estimations of round-trip times caused by path asymmetry that can occur in VANETs. [Men+18, pp. 34-35]

UDP faces problems with detecting disconnected recipients. As a result, UDP senders might continue to send packets to unreachable recipients and therewith waste bandwidth of intermediate nodes for a significant time. [Men+18, pp. 34-35]

To have a better performing transport protocol, protocols, such as the vehicle transport protocol (VTP) by Schmitz et al. [Sch+06] and the mobile control transport protocol (MCTP) by Bechler et al. [Bec+05], have been proposed specifically for the usage in VANETs. These base on similar principles as ad hoc TCP by Liu and Signh [LS01a]. However, these and many other academically proposed VANET transport protocols are designed for Unicast routing. [Men+18, pp. 34-35]

Application Layer

In common VANET standard sets, the application layer is specific to the respective standard set and its applications (e.g., in ETSI C-ITS an application layer is specified, while in WAVE no application layer is specified [Fes15]). Application layer protocols should minimize end-to-end delay for all ITS applications, especially for road safety applications where real-time deadlines might have to be complied with [Cun+16].

3.3 Intelligent Transport Systems Applications

Road safety is one of the major potential improvements that drives ITS [Ham+15]. ITS and their applications are expected to significantly reduce the number of traffic accidents [Ham+15]. Traffic accidents are discussed in more detail in section 9.7 Traffic Accidents in Traditional Traffic Environments and Vehicular Ad Hoc Networks.

ITS applications have been categorized by Rasheed et al. [Ras+17] as follows.

3.3.1 Road Safety Applications

Road safety applications in VANETs aim to increase road safety by warning drivers of Smart Vehicles early, therefore allowing a timely response to potentially dangerous situations. These applications try to achieve this via the distribution of information about hazards and obstacles. For example, multiple Smart Vehicles are driving lined up close to each other and the foremost Smart Vehicle in such a lineup performs an emergency brake. For an emergency brake, the driver has to significantly depress the brakes, which is detected by the driver's Smart Vehicle. The foremost Smart Vehicle then automatically warns the drivers of the following Smart Vehicles. Ideally, this warning allows the drivers of the following Smart Vehicles to react significantly faster and potentially avoid a traffic accident. For this to be effective it is critical to satisfy a strict time delay. [Ras+17]

The critical latency for road safety applications is 100ms [Ham+15].

3.3.2 Traffic Control and Management Applications

Traffic control and management applications aim to optimize traffic flows and minimize travel time by avoiding traffic congestions or assisting drivers with optimal route selection. Examples for such applications are automatic toll fee payment or intelligent traffic signals that adapt their green phases to the traffic situation. [Ras+17]

The critical latency for traffic control and management applications is between 100ms and 200ms, depending on the exact application. [Ham+15]

3.3.3 Comfort and Infotainment Applications

Comfort and infotainment applications aim to increase driving comfort and provide entertainment to travelers. Use cases include internet-based services, such as video streaming and location-based information, such as the location of the closest restaurant. [Ras+17]

The critical latency for infotainment and comfort applications is 500ms. [Ham+15]

CHAPTER 4

ETSI Cooperative Intelligent Transport Systems Standard Set

This chapter describes the most notable elements of ETSI C-ITS. It contains an overview of the standard set layout and the entire ETSI C-ITS stack.

4.1 Overview

To introduce ITS on a large scale, ETSI has developed a VANET standard set in collaboration with the Comité Européen de Normalisation (CEN) and the ISO [Fes15]. The release 1 of the resulting standard set is defined in ETSI Technical Report (TR) 101 607 V1.1.1 – Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1 [Ins13b]. The standard set is also known as ETSI C-ITS [CE14] or simply C-ITS [Fes15]. This thesis focuses on the release 1 of ETSI C-ITS.

ETSI C-ITS consists of horizontal layers for access technologies, networking and transport, facilities, and applications. Furthermore, ETSI C-ITS has vertical layers for management and security. An overview of the protocol stack is displayed in Figure 12. [Fes15]

4.2 Access Technologies

ETSI C-ITS summarizes the physical layer and the data link layer under the name access technologies [Fes15]. These access technologies are commonly known as Intelligent Transport Systems in the 5 GHz frequency band (ITS-G5) and are based on the 802.11p wireless communication standard [Fes15].

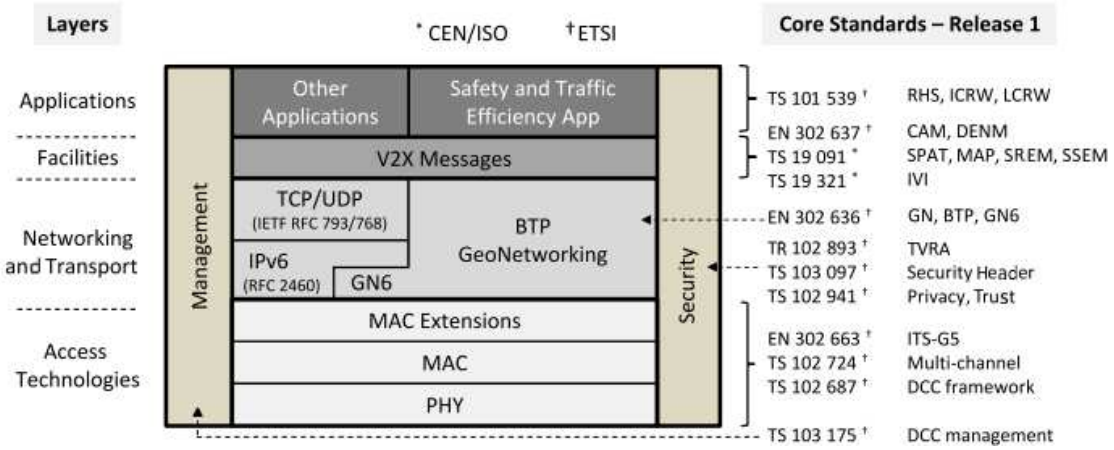


Figure 12: ETSI C-ITS Protocol Stack cf. [Fes15]

4.2.1 Physical Layer

The physical layer (PHY) of ETSI C-ITS is based on a radio frequency band [Ins12b]. This frequency band is divided into parts A to D as follows [Ins12b]:

- Band A of ITS-G5 (ITS-G5A) is the primary frequency band with a bandwidth of 30 MHz and is dedicated to ITS road safety applications and traffic control applications. ITS-G5A has three channels (Service Channel (SCH) 1 ch 176, SCH2 ch 178, and Control Channel (CCH) ch 180), each with 10 MHz channel bandwidth, equally distributed over a spectrum between 5875 and 5905 MHz. [Ins12b]
- Band B of ITS-G5 (ITS-G5B) has a frequency band with a 20 MHz spectrum for non-road-safety and non-traffic-control applications. These applications communicate on two channels (SCH4 ch 172, SCH3 ch 174), each with a 10 MHz spectrum, distributed over 5855-5875 MHz. [Ins12b]
- In band C of ITS-G5 (ITS-G5C), a bandwidth of 255 MHz is available for shared usage with Radio Local Area Networks (RLANs) distributed over a spectrum between 5470 and 5725 MHz. [Ins12b]
- Band D of ITS-G5 (ITS-G5D) is dedicated to the future usage of ITS applications and consists of two channels (SCH5 ch 182, SCH6 ch 184), each with a bandwidth of 10 MHz, distributed over a spectrum between 5905 and 5915 MHz. [Ins12b]

Figure 13 displays the ITS-G5 frequency band. This frequency band can also be used by the cellular communication-based Long-Term Evolution (LTE)-V2X standard by the Third Generation Partnership Project (3GPP) that was recently standardized in the Release 2 of ETSI C-ITS [Ins20].

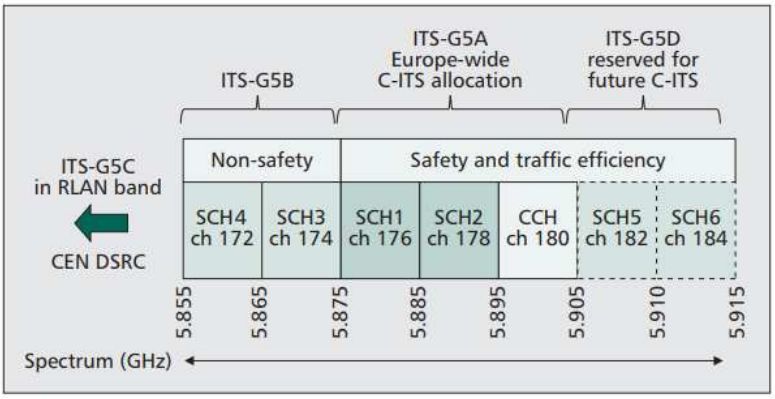


Figure 13: ITS-G5 Frequency Band (c.f. [Fes14])

4.2.2 Data Link Layer

The data link layer of ETSI C-ITS is subdivided into the MAC and the LLC layer [Ins19]. The lower MAC layer of ETSI C-ITS is further extended by an upper MAC layer, also known as the MAC extensions layer [Fer+18].

4.2.3 Lower MAC Layer

The lower MAC layer is responsible for scheduling transmissions to minimize interference between ITS stations and increase packet reception probability. CSMA/CA [Gal85] is used as MAC layer protocol. The collision avoidance algorithm is the Enhanced Distributed Coordination Access (EDCA) algorithm. As discussed in subsection 3.2.3 Vehicular Ad Hoc Networks, CSMA algorithms belong to the category of contention-based protocols. EDCA extends this behavior by adding QoS and allows the MAC layer to prioritize certain traffic. To prioritize traffic, high priority traffic is given a higher likelihood of access to the channel than low priority traffic. [Ins19]

4.2.4 MAC Extensions Layer

The MAC extensions layer extends the MAC layer with multi-channel operation and a *gatekeeper* entity – the Decentralized Congestion Control's (DCC) [Fes14].

The DCC is a management entity that regulates network load. It does not aim to achieve interoperability but is merely an entity that ensures a single entity does not consume all resources of a channel. Notably, the DCC is not a security measure, but a QoS measure. [Ins19]

Though the DCC functionality mainly resides in the MAC extensions layer, it is also distributed around the access layer, the network layer, the transport layer, the facilities layer, and the management layer. [Ins18d]

Figure 14 shows the distribution of the DCC across all layers.

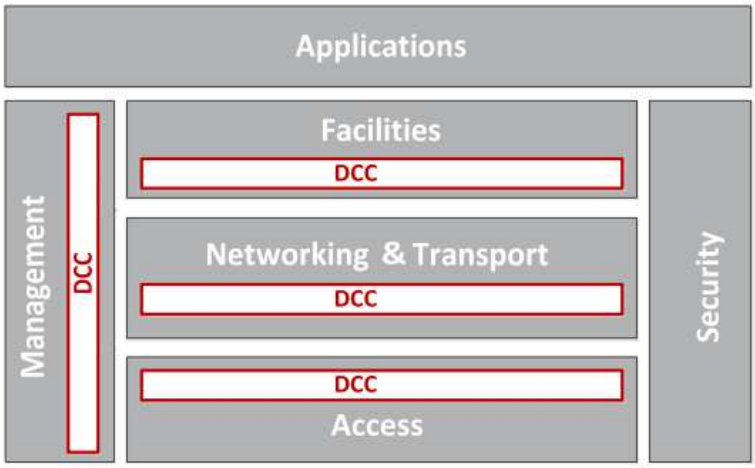


Figure 14: DCC Cross-Layer Distribution (c.f. [Ins18d])

4.2.5 Logical Link Control Layer

The LLC layer is responsible for distinguishing different network protocols, such as GeoNetworking or GeoNetworking over IPv6 (GN6) [Sjö+16]. GeoNetworking and GeoNetworking over IPv6 are both described in the following section.

4.3 Network and Transport Layer

On the network and transport layer, ETSI C-ITS essentially consists of two different stacks: the IPv6 over GeoNetworking (GN6) stack and the GeoNetworking stack [Fes15]. These stacks are described in the following subsections.

ETSI C-ITS collectively describes the combination of Smart Vehicles and RSU's as *ITS station*. Such a combination is referred to as *ITS station* in the following.

4.3.1 Network Layer

Possible network protocols for ETSI C-ITS communication are: GeoNetworking, IPv6 via GeoNetworking, IPv6 with mobility support, and Communications Access for Land Mobiles (CALM) [Ins10b]. However, only GeoNetworking and GN6 have specifically been addressed in more detail throughout ETSI C-ITS (e.g., in ETSI EN 302 636-1 [Ins14a], in ETSI EN 302 636-3 [Ins14b], in ETSI EN 302 636-2 [Ins13a], or in ETSI EN 303 613 [Ins14c]).

GeoNetworking Protocol

The GeoNetworking protocol allows communication with one ITS station at a geographic location, or one or more ITS stations in a geographic target area. The GeoNetworking

protocol employs geographic addressing and geographic forwarding. As such, it is responsible for geographically-based communication. [Fes15]

The GeoNetworking protocol consists of various information dissemination paradigms. An overview of the information dissemination paradigms is displayed in Table 1. For the description of the information dissemination paradigms the following terminology is used:

- Sender – A sender of a packet.
- Forwarder – A forwarder of a packet.
- Intermediary Recipient – An intermediary recipient of a packet, i.e., a recipient that is not the final recipient of a packet.
- Destination – The final destination/recipient of the packet.

Single-Hop Broadcast: In Single-Hop Broadcast (SHB) messages are broadcasted in a single-hop, to all neighbors of the sending ITS station. [Ins11b]

Topologically Scoped Broadcast: Topologically Scoped Broadcast (TSB) is similar to SHB. However, instead of a single-hop, messages are retransmitted by recipients to all their neighbors until the messages have hopped n times [Ins11b]. The forwarding of messages in n hops is further referred to as N-Hop Broadcast Forwarding (NHBF).

GeoUnicast: GeoUnicast is used if an ITS station X wants to send a message to another ITS station Y at a geographic location. If Y's location is unknown to X, X invokes the Location Service (LS) to obtain Y's location. Otherwise, the sending ITS station shall forward the message with one of the forwarding algorithms *Greedy Forwarding* (GF) or *Contention-Based Forwarding* (CBF). [Ins11b]

In GF, the selection of an optimal forwarder is done at the sender. A sender of a GF packet uses the destination information in the packet header to select one of its neighbors as the next hop, unless the destination of the packet is in the immediate neighborhood of the sender. Neighbor selection is done via the Most Forward within Radius (MFR) strategy by Takagi and Kleinrock [TK84]. MFR selects the neighbor with the smallest geographic distance to the destination as an optimal forwarder. The geographic distance to the destination is taken from a sender's location table. When the destination is in the immediate neighborhood of the sender, the sender simply sends the packet to the destination. [Ins11b]

Though not explicitly referenced in ETSI C-ITS, CBF, as used in ETSI C-ITS, appears the be identical to CBF by Füßler et al. [Füß+03; Fü+04].

In CBF, the selection of an optimal forwarder is done at the intermediary recipients. A sender of a CBF packet sends the packet by broadcasting it to all its neighbors. Every intermediary recipient buffers the packet and starts a timer that is inversely proportional to the distance between the intermediary recipient's location and the destination's

Paradigm	**Forwarding**	**Phase**
Single-Hop Broadcast	No forwarding	Broadcast
Topologically Scoped Broadcast	*N*-Hop Broadcast Forwarding	Broadcast
GeoUnicast	Greedy Forwarding or Contention-Based Forwarding	Unicast based on geographic location
GeoAnycast	Greedy Forwarding or Contention-Based Forwarding	Unicast based on geographic area
GeoBroadcast	Simple GeoBroadcast Forwarding	GeoUnicast (situational): Greedy Forwarding
		GeoBroadcast: Broadcast forwarding based on geographic area (i.e., GeoBroadcast Forwarding)
	Advanced GeoBroadcast Forwarding 1 (Experimental)	GeoUnicast (situational): Greedy Forwarding and Contention-Based Forwarding
		GeoBroadcast: GeoBroadcast Forwarding with a retransmission scheme
	Advanced GeoBroadcast Forwarding 2 (Experimental)	GeoUnicast (situational): Contention-Based Forwarding
		GeoBroadcast: GeoBroadcast Forwarding with a sectorial suppression scheme

Table 1: Overview of Dissemination Paradigms in ETSI C-ITS [Ins11b]

location. Upon expiration of an intermediary recipient's timer, the intermediary recipient re-broadcasts the packet. This re-broadcasting may let an ITS station which already received the packet once receive it another time. In this case, the ITS station stops its timer and removes the packet from their buffer, since it knows that another ITS station had a shorter timer and as a result, is closer to the destination. The ITS station that first rebroadcasts the packet is considered to be the optimal forwarder. CBF has an implicit reliability mechanism. A packet is implicitly forwarded by any ITS station that received the packet in case one or multiple ITS stations with shorter retransmission timers do not forward the packet (e.g., due to connection problems). In comparison to GF, CBF has a larger forwarding delay and requires additional processing. [Ins11b]

While GF with MFR requires beacons to function, CBF can function beaconless [Fü+04].

GeoAnycast: GeoAnycast enables an ITS station to send a message to a single ITS station

within a geographic target area. Packets in GeoAnycast can be forwarded either by GF or by CBF. Upon reception of a GeoAnycast packet, a recipient determines whether it is located inside, at the border, or outside of the geographic target area. If the recipient is located inside the geographic target area, the recipient does not forward the packet but instead passes it to the upper layers for processing. Otherwise, the recipient forwards the packet. [Ins11b]

GeoBroadcast: GeoBroadcast allows an ITS station to send a message to all ITS stations within a geographic target area [Ins11b]. Analogously to GeoAnycast, in GeoBroadcast it is determined whether a recipient is located inside, at the border, or outside of the geographic target area. This process is described later in this subsection.

Forwarding in GeoBroadcast can be enabled through three different algorithms: Simple GeoBroadcast Forwarding, Advanced GeoBroadcast Forwarding 1, and Advanced GeoBroadcast Forwarding 2 [Ins11b]. The algorithms Advanced GeoBroadcast Forwarding 1 and 2 are not standardized yet and are only included in ETSI Technical Specification (TS) 102 636-4-1 [Ins11b] for informative purposes.

The GeoBroadcast forwarding algorithms comprise of two phases: the GeoUnicast phase and the GeoBroadcast phase. This thesis describes the functionality of the GeoBroadcast forwarding algorithms with these phases.

In Simple GeoBroadcast Forwarding, it is first determined whether an ITS station is located inside, at the border, or outside of the geographic target area of a Simple GeoBroadcast Forwarding packet [Ins11b]. (1) If the ITS station is outside of the target area, the packet is forwarded with GF as specified for GeoUnicast [Ins11b]. (2) If the ITS station is inside or at the border of the target area, the packet shall be forwarded with GeoBroadcast Forwarding (GBF; i.e., be rebroadcasted) [Ins11b]. In this thesis, case (1) is called *situational GeoUnicast phase* and case (2) is described as *GeoBroadcast phase*.

Though ETSI TS 102 636-4-1 [Ins11b] does not specify how Advanced GeoBroadcast Forwarding 1 and 2 determine whether an ITS station is located inside, at the border, or outside of the geographic target area of an Advanced Geobroadcast Forwarding 1/2 packet, it would be reasonable to expect that this determination would happen analogously to Simple GeoBroadcast Forwarding.

Advanced GeoBroadcast Forwarding 1 uses three main mechanisms [Ins11b]:

- GF to minimize forwarding delay (situational GeoUnicast phase). [Ins11b]
- CBF to deal with communication failures (situational GeoUnicast phase). [Ins11b]
- A controlled packet retransmission scheme to improve the reliability of the dissemination process within the geographic target area (GeoBroadcast phase). [Ins11b]

The combination of GF and CBF improves the reliability and latency of GeoUnicast by avoiding the communication problems of GF and the delay of CBF. The retransmission scheme in the GeoBroadcast phase provides increased reliability of Advanced

GeoBroadcast Forwarding 1 when compared to the GeoBroadcast phase of Simple GeoBroadcast Forwarding by enabling redundant retransmissions. The number of redundant transmissions can be configured through a threshold. [Fes14]

Advanced GeoBroadcast Forwarding 2 uses two main mechanisms [Ins11b]:

- CBF to deal with communication failures (situational GeoUnicast phase). [Ins11b]
- A sectoral suppression algorithm designed by Mariyasagayam et al. [Mar+07] to improve connectivity (GeoBroadcast phase). [Ins11b]

In the employed sectoral suppression algorithm, a rebroadcaster is selected based on its relative location to the sender. Similar to CBF, based on the distance between the sender of a message, a potential rebroadcaster starts a retransmission timer. In case the distance is above a certain maximum distance threshold, a potential rebroadcaster refrains from forwarding the message. If the potential rebroadcaster receives the initial message again before the retransmission timer expires, it will refrain from rebroadcasting the message. Otherwise, the ITS station rebroadcasts the message on the expiration of the retransmission timer. [Mar+07]

Most well-known VANET routing protocols only have one forwarding algorithm (e.g., AODV [PR99], Dynamic Source Routing (DSR) by Johnson and Malz [JM96], Optimized Link State Routing (OLSR) by Clausen et al. [Cla+03], Temporally Ordered Routing Protocol (TORA) by Park and Corson [PC97], or Destination-Sequenced Distance Vector (DSDV) by Perkins and Bhagwat [PB94]). Unlike most well-known VANET routing protocols, the GeoNetworking protocol has multiple forwarding algorithms [Ins11b]. More specifically, the GeoNetworking has the forwarding algorithms: NHBF, GF, CBF, GBF, GBF with a packet retransmission scheme, and GBF with a sectoral suppression algorithm [Ins11b]. Some of these forwarding algorithms function fundamentally differently. For example, in GF a recipient of a packet immediately retransmits the packet to the optimal forwarder, while in CBF a recipient retransmits a packet after expiration of a retransmission timer and only if they have not received the packet another time [Ins11b]. As a result of this different functionality, research on the GeoNetworking protocol may have to consider the forwarding algorithms of the GeoNetworking protocol individually. For example, a performance analysis of the GeoNetworking protocol will have to consider each forwarding algorithm of the GeoNetworking protocol individually. Otherwise, the performance analysis would neglect the different performances of the forwarding algorithms [Ins11b].

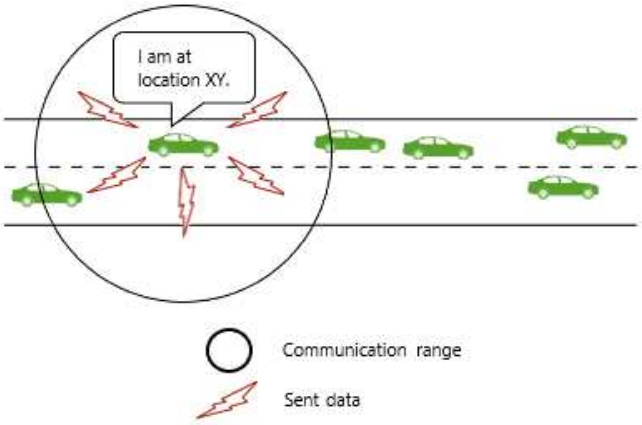


Figure 15: Beaconing in ETSI C-ITS (cf. [Men+18, pp. 32–34])

The dissemination paradigms of the GeoNetworking protocol are supported by the following network features:

- Beaconing [Ins11b]
- Store-Carry-Forward [Lla+15]
- Location Service [Ins11b]

Beaconing: Beacon messages are periodically sent by ITS stations to advertise their location vector to other ITS stations via SHB [Ins11b]. Figure 15 displays the concept of beaconing. In contrast to much other GeoNetworking functionality (e.g., GeoUnicast, GeoAnycast, or GeoBroadcast), these beacons do not carry a payload of a higher layer of ETSI C-ITS (e.g., the facilities layer) [Ins11b]. The location vectors of beacons are processed by receiving ITS stations and stored in their location table [Ins17a]. Storing location vectors allows ITS stations to determine the positions of neighboring ITS stations [Ins17a]. To update location vectors of IT stations, as described in ETSI EN 302 636-4-1 [Ins17a], it is required to have one or multiple identifiers that uniquely identify an ITS station. Though not explicitly stated in ETSI EN 302 636-4-1 [Ins17a], the unique identifier for the location table is presumably the GeoNetworking address. Other data elements of the location table, such as the logical link address, the type of ITS station, or the version of the GeoNetworking protocol, are either included in the GeoNetworking address or would not constitute a unique identifier. By default, there are no security measures to ensure that beacons are authentic [Ins17a].

Store-Carry-Forward: The GeoNetworking protocol employs a technique called Store, Carry, and Forward (SCF). This technique is used in environments where a next-hop

is not possible (e.g., due to low traffic density). SCF enables storing a GeoNetworking packet until a next-hop is available. [Lla+15]

Location Service: With the LS, an ITS station can determine the location of another ITS station. A location is determined when an ITS station wants to send a message to another ITS station but does not have the corresponding location in its location table. To determine the location of another ITS station, an ITS station sends an LS Request. The LS Request is forwarded to intermediary recipients via TSB until it reaches the target ITS station. This ITS station then answers with its location through an LS Reply via GeoUnicast. [Ins11b]

Internet Protocol Version 6 over GeoNetworking

In ETSI C-ITS, there is an adaption of the GeoNetworking protocol that supports IPv6. This adaption is known as GN6 [Fes14]. To support IPv6, the GeoNetworking protocol provides the upper layers of the ETSI C-ITS stack with a sub-IP multi-hop delivery mechanism [Ins14c]. GN6 is based on traditional IP-addressing and geographic forwarding [Fes14]. This allows traditional IPv6 communication with arbitrary IPv6 hosts, within ETSI C-ITS or on the internet [Fes14]. The IPv6 communication within ETSI C-ITS is limited to IPv6 multicast and IPv6 anycast [Ins14c].

4.3.2 Transport Layer

The transport layer of ETSI C-ITS consists of the Basic Transport Protocol (BTP) and TCP/UDP. The BTP resides on the GeoNetworking stack, while TCP/UDP resides on the GN6 stack.

Basic Transport Protocol

BTP is a connection-less protocol that enables communication between the ITS stations [Fer+18]. BTP is a best-effort transport protocol similar to UDP [CE14]. It does not guarantee the transmission of a packet [CE14]. On the facilities layer Cooperative Awareness Messages (CAMs, Distributed Environmental Notification Messages (DENMs), MAP, and Signal Phase and Time (SPAT) use BTP [Ins14d].

Transport Control Protocol/User Datagram Protocol the via Internet Protocol Version 6 over GeoNetoworking

In ETSI C-ITS, the IPv6 protocol is used in combination with TCP/UDP for non-road-safety application [Fes15].

4.4 Facilities Layer

ETSI C-ITS has a facilities layer in its stack [Ins10b]. The facilities layer contains predefined V2X messaging and V2I/I2V messaging including V2I/I2V services [Ins18c].

4.4.1 Vehicle-To-Anything Messaging

V2X messaging in ETSI C-ITS heavily relies on CAM and DENM [Fes15]. CAMs are very important in ETSI C-ITS because they periodically communicate critical vehicle information (e.g., vehicle speed) to support road safety, traffic control, and traffic management applications [Fes15]. DENMs publish road-safety information based on a geographic target area [Ker+16]. DENM transmissions are specifically initiated by applications [Fes15].

4.4.2 Vehicle-To-Infrastructure Messaging

ETSI C-ITS provides various dedicated V2I/I2V message types out-of-the-box. They are as follows [Ins12b]:

- Signal Phase and Timing Extended Message (SPATEM) – SPATEMs hold information about signal phases and timing of traffic light RSUs. They are periodically sent by traffic light RSUs via GeoBroadcast. [Ins12b]
- MAP Extended Message (MAPEM) – MAPEMs contain changes in the topology of traffic infrastructure (e.g., traffic deviation). They are sent by RSUs via GeoBroadcast. As the topology of traffic infrastructure is rather static, MAPEMs are sent relatively seldom. [Ins12b]
- Infrastructure-to-Vehicle Information Message (IVIM) – IVIMs enable mandatory and advisory road signage. Among such signage are contextual speeds and road works warnings. Information is disseminated via SHB or GeoBroadcast based on a Minimum Dissemination Area (MDA). If the MDA is smaller than the SHB range, SHB is used. Otherwise, GeoBroadcast is used. [Ins12b]
- Signal Request Extended Message (SREM) – SREMs are used to request prioritization of public transport and public safety vehicles at signalized road infrastructure, such as intersections. SREMs are disseminated via GeoBroadcast. [Ins12b]
- Signal Request Status Extended Message (SSEM) – SSEMs are sent in response to SREMs. An SSEM notifies the sender of an SREM if their request has been granted, canceled, or changed in priority (e.g., due to a more relevant SREM from an ambulance). SSEMs are disseminated via GeoBroadcast. [Ins12b]
- Radio Technical Commission for Maritime Services (RTCM) Extended Message (RTCMEM) – RTCMEMs enable various types of location corrections (e.g., for GPS). Stationary Global Navigation Satellite System (GNSS) base stations generate RTCM correction data. This data is used to correct the positions of mobile GNSS stations (e.g., cars). RTCMEMs are disseminated via GeoBroadcast. [Ins12b]

4.4.3 Vehicle-to-Infrastructure/Infrastructure-to-Vehicle Services

ETSI C-ITS has various V2I/I2V services. These are: Traffic Light Maneuver (TLM), Road and Lane Topology (RLT), Infrastructure-to-Vehicle Information (IVI), Traffic Light Control (TLC), and GNSS Positioning Correction (GPC). [Ins18c]

The TLM service uses SPATEMs and supports the execution of safe maneuvers at intersections. It informs traffic participants about the operational states of traffic lights, the current signal state, the residual time of the current state before changing to the next state, the allowed maneuvers and assists crossings. [Ins18c]

The RLT service uses MAPEMs and informs about the topology of traffic infrastructure. This information includes the road and lane topology and the allowed maneuvers within an intersection area or a road segment. [Ins18c]

The IVI service uses IVIMs. The IVI service provides mandatory and advisory road signage (e.g., contextual speeds or road works warnings). [Ins18c]

The TLC service uses SREMs and SSEMs. The TLC service enables the prioritization of public transport or public safety vehicles on signalized road infrastructure (e.g., intersections). Not only can this functionality be used for a single signalized road infrastructure, but also for a sequence of signalized road infrastructure (e.g., intersections along a route).

The GPC service uses RTCMEMs messaging and performs location correction for GNSS stations as defined by the RTCM. [Ins18c]

4.5 Application Layer

ETSI C-ITS defines a basic set of applications. This definition consists of a categorization of use cases into applications and a categorization of applications into application classes. Notably, the use cases and applications defined in ETSI TR 102 638 [Ins09] are not up-to-date anymore as they have been partly and implicitly superseded by the definition of the applications Road Hazard Signalling (RHS) in ETSI TS 101 539-1 [Ins13c], Intersection Collision Risk Warning (ICRW) in ETSI TS 101 539-2 [Ins18a], and Longitudinal Collision Risk Warning (LCRW) in ETSI TS 101 539-3 [Ins13d].

Table 2 provides an overview of the basic set of applications as defined in ETSI TR 102 638 [Ins09] including the implicit updates in ETSI TS 101 539-1 [Ins13c], ETSI TS 101 539-2 [Ins18a], and ETSI TS 101 539-3 [Ins13d].

The main objective of the active road safety class is the improvement of road safety. The cooperative traffic efficiency class aims to increase the fluidity of traffic. The classes *cooperative local services* and *global internet services* aim to advertise and provide on-demand information to passing Smart Vehicles. This advertisement/information can be commercial or non-commercial, and can include infotainment, comfort, vehicle management, and service lifecycle management. Only active road safety applications have been standardized in ETSI C-ITS yet. [Ins09]

Application Class	Application	Use Case
Active road safety	RHS	Emergency vehicle approaching
		Slow vehicle
		Stationary vehicle
		Emergency electronic brake lights
		Wrong way driving
		Adverse weather condition
		Hazardous location
		Traffic condition
		Roadwork
		Human presence on the road
	ICRW	Crossing collision
		Traffic sign violation
		Collision involving vulnerable road users
		Rear end collision
	LCRW	Forward collision
		Forward/side collision
		Frontal collision
Cooperative traffic	Speed management efficiency	Regulatory/contextual speed limits notification
		Traffic light optimal speed advisory
	Cooperative navigation	Traffic information and recommended itinerary
		Enhanced route guidance and navigation
		Limited access warning and detour notification
		In-vehicle signage
Cooperative local	Location based services services	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet	Communities Services services	Insurance and financial services
		Fleet management
		Loading zone management
	ITS station life cycle management	Vehicle software/data provisioning and update
		Vehicle and RSU data calibration

Table 2: Basic Set of Applications [Ins09] with Updated Information of ETSI TS 101 539-1 [Ins13c], ETSI TS 101 539-2 [Ins18a], and ETSI TS 101 539-3 [Ins13d]

Standard	Used Version	Topic
ETSI TR 102 893	V1.2.1	Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
ETSI TS 102 940	V1.3.1	Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management
ETSI TS 102 941	V1.3.1	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 102 942	V1.1.1	Intelligent Transport Systems (ITS); Security; Access Control
ETSI TS 102 943	V1.1.1	Intelligent Transport Systems (ITS); Security; Confidentiality Services
ETSI TS 103 097	V1.3.1	Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats

Table 3: ETSI C-ITS Security Standards [Ins13b]

The applications disseminate information based on CAM and DENM on the facilities layer [Ins09]. This means that, for example, ICRWs are disseminated via CAMs and/or DEMs.

4.6 Security Layer

The following section aims to give an overview of the security standards of ETSI C-ITS. For detailed information it is referred to the respective standard. The security standards are displayed in Table 3 [Ins13b]. Notably, ETSI TS 102 867 has apparently been silently removed from the standard set, as it is not available on ETSI's website anymore [Ins].

4.6.1 Threat, Vulnerability, and Risk Analysis

ETSI TR 102 893 [Ins17b] provides an overview of the security of ETSI C-ITS and presents the results of a Threat, Vulnerability, and Risk Analysis (TVRA) of the 5.9 GHz frequency band in an ITS. The scope of the analysis is V2V and V2I/I2V data and services. Most importantly, ETSI TR 102 893 tries to list all potential threats to ITS stations and countermeasures against all discovered threats.

Some of the listed threats are mitigated or prevented through security measures specified in ETSI TS 102 940 [Ins18b], ETSI TS 102 941 [Ins10c], ETSI TS 102 942 [Ins12c], ETSI TS 102 943 [Ins12d], and ETSI TS 103 097 [Ins17d]. Examples for security measures are

use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle and *digitally sign each message using a Kerberos/PKI-like token system.*

4.6.2 Technical Specifications of Security Standards

In ETSI TS 102 940 [Ins18b], the security architecture for ITS communication is specified. The functional entities and their interconnection required to support security in ETSI C-ITS are identified (e.g., the connection between the management layer and the security layer), as well as roles (e.g., Smart Vehicles or RSUs) and locations for multiple security services (e.g., a service to send secured messages or a service to encrypt a single message). These security services protect transmitted information and manage security parameters. To support these services identifier and certificate management, PKI processes and interfaces, and basic principles (e.g., protection of shared information within ETSI C-ITS) and guidelines (e.g., keys should be exchanged in an encrypted form) for trust establishment are defined.

ETSI TS 102 941 [Ins10c] consists of the specification of trust and privacy management. These specifications include a description of measures to ensure privacy (e.g., pseudonymity), ITS station life-cycle management (i.e., from the manufacture of an ITS station to its end-of-life), the management of PKI, and the generation, distribution, and use of trust information lists.

In ETSI TS 102 942 [Ins12c] authentication and authorization services are specified. These services prevent unauthorized access to other services (e.g., by providing basic CAM authorization or authorization for hazard warnings).

ETSI TS 102 943 [Ins12d] covers the specification of confidentiality requirements (e.g., the non-necessity of confidentiality in CAMs) and confidentiality services (e.g., a confidentiality service for IPv6). These services shall ensure that information sent to and from an ITS station is sufficiently confidential for the participating parties.

Arguably, ETSI TS 102 940 [Ins18b], ETSI TS 102 941 [Ins10c], ETSI TS 102 942 [Ins12c], and ETSI TS 102 943 [Ins12d] are all strongly focused to securely support the functionality of the ETSI C-ITS security header that is defined in ETSI TS 103 097 [Ins17d]. ETSI TS 103 097 mainly consists of the specification of secure data structures including the ETSI C-ITS security header and certificate formats for ETSI C-ITS. The ETSI C-ITS security header provides confidentiality, integrity, and authenticity to the GeoNetworking Common Header and the upper layer payload (e.g., a CAM or DENM payload) through a signature and/or encryption [Ins11b].

The security architecture in ETSI C-ITS can be described as a hybrid PKI-/Kerberos-like system. This system is displayed in Figure 16. With its self-signed Bootstrap Certificate (BC), a Smart Vehicle can obtain Enrollment Credentials (ECs) from an Enrollment Authority (EA) [Ins18b]. With these ECs, the Smart Vehicle can obtain Authorization Tickets (ATs) from an Authorization Authority (AA) [Ins18b]. These ATs can, in turn, be used to secure messages with an ETSI C-ITS security header [Ins18b].

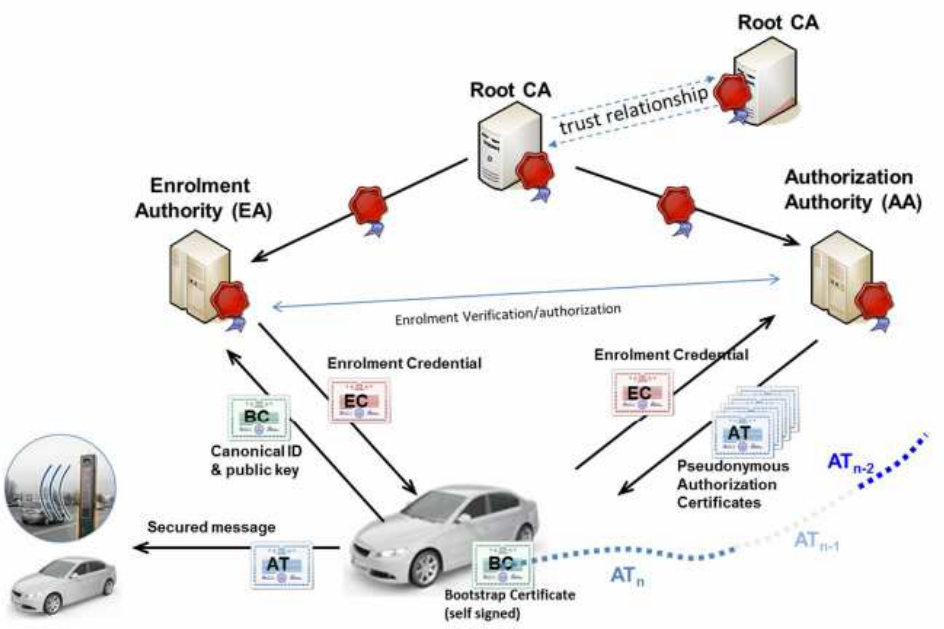


Figure 16: ETSI C-ITS Security Architecture [Ins18b]

This process provides pseudonymity to ETSI C-ITS users and at the same time, allows accountability [Ins18b]. The provided pseudonymity aims to protect the privacy of ETSI C-ITS users and shall prevent attacks on privacy, such as location tracking attacks [Ins17b]. The process of obtaining enrollment credentials and pseudonym certificates is comparable with ticketing in Kerberos [Mil+87]. Both the EA and the AA have one or multiple root Certificate Authorities (CAs) as root(s) of trust [Ins18b]. This is an adaptation of traditional PKI [KL14, pp. 474-476].

Haidar et al. [Hai+19] perform a risk analysis of ETSI C-ITS pseudonymity. The risk analysis methodology follows ETSI TR 102 165-1 version 5.2.3 [Ins17c]. The authors consider threat agents with programmable radio frequency receivers (i.e. eavesdroppers) and threat agents with keying material that allows them to pose as a valid Smart Vehicle. Among well-known attacks on pseudonyms in VANETs, such as location tracking attacks, alteration of trust anchor information, and false message injection [SAR17], the authors propose two new attacks: pseudonym change strategy inhibition and exhaustion of the pseudonym pool. The former is an attack where an attacker blocks the pseudonym change of a genuine Smart Vehicle. The latter attack aims to exhaust the pseudonym pool of a genuine Smart Vehicle by remotely triggering pseudonym changes. The authors identify a critical risk for Sybil attacks, location tracking attacks, false message injection, alteration of trust anchor information, and exhaustion of the pseudonym pool. Minor risk is found for pseudonym change strategy inhibition.

Nowdehi and Olovsson [NO14] and Nowdehi [Now13] conduct empirical research on ETSI

Standard	Used Version	Topic
ETSI TS 103 096-1	V1.4.1	Intelligent Transport Systems (ITS); Testing; Conformance Test Specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)
ETSI TS 103 096-2	V1.4.1	Intelligent Transport Systems (ITS); Testing; Conformance Test Specifications for ITS Security Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 103 096-3	V1.4.1	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)

Table 4: ETSI C-ITS Security Conformance [Ins13b]

TS 103 097 [Ins17d]. During the implementation of ETSI TS 103 097, they identify design flaws in the specifications that lead to potential vulnerabilities in an implementation of the ETSI C-ITS security header. One design flaw allows multiple payloads in CAMs and DENMs. This may result in vulnerabilities in the signature verification and makes parsing rather complicated. Another design flaw allows using arbitrarily long values for the *length of the length* field of an ETSI C-ITS security header. This design flaw is likely to lead to memory corruption vulnerabilities in implementations of the ETSI C-ITS security header.

Such memory corruption vulnerabilities could be used to perform attacks on Smart Vehicles, as described in section 9.2 Vehicular Security.

4.6.3 Security Standard Conformance

An ETSI C-ITS implementation has to conform to the TS' listed in Table 3 and pass security tests specified in the security testing standards as displayed in Table 4. The specified security tests in these security testing standards validate the functionality of ETSI TS 103 097 [Ins17d]. There are no security testing standards that cover security tests for other security measures [Ins]. For example, there are no security testing standards for *provide remote deactivation of misbehaving devices capability* or *limit message traffic to V2I/I2V when infrastructure is available and implement message flow control and station registration*, both of which are *recommended* security measures in ETSI TR 102 893 [Ins17b].

4.7 Management Layer

The management layer in ETSI C-ITS mainly consists of DCC management. DCC management handles the DCC on the facilities layer, the networking layer, transport layer, and the access layer. DCC management evaluates the current load on the ITS-G5 radio channels and optimizes the load by adjusting DCC parameters. [Ins15]

For evaluating and optimizing load, the DCC uses profiles. DCC profiles are applied depending on the state of the channels ITS-G5A and ITS-G5B. DCC profiles restrict channel access by restricting the transmit power and the message rate of ITS stations. [Ins12b]

CHAPTER 5

Security of Vehicular Ad Hoc Networks and their Network Layer

This chapter covers the security characteristics of VANETs by describing the security requirements and security challenges of VANETs. Due to this thesis' focus on black hole attacks, which happen on the network layer, an overview of network layer attacks is given later in this chapter. Black hole attacks themselves are discussed in detail in the next chapter.

5.1 Security Requirements and Related Challenges

As discussed in subsection 3.2.3 Vehicular Ad Hoc Networks, VANETs are a subgroup of MANETs. As a result, many security characteristics of VANETs are inherited from MANETs [Qu+15]. However, unlike many general-purpose MANETs (e.g., iMANETs) and other traditional IT systems (e.g., desktop PCs or TVs), VANETs are safety-critical systems, in which attacks can have fatal consequences [Qu+15]. As a result, security is crucial in VANETs.

In current research, there are several categorizations of security requirements of VANETs (e.g., by Hasrouny et al. [Has+17] or by Qu et al. [Qu+15]). The categorization in this thesis is based on the security requirements defined in chapter 2 Fundamentals of IT Security. Figure 17 depicts the security properties of VANETs.

The IT security of modern vehicles, in general, is described in section 9.2 Vehicular Security. The relation between VANETs, VANET security, and traffic accidents is described in more detail in section 9.7 Traffic Accidents in Traditional Traffic Environments and Vehicular Ad Hoc Networks.

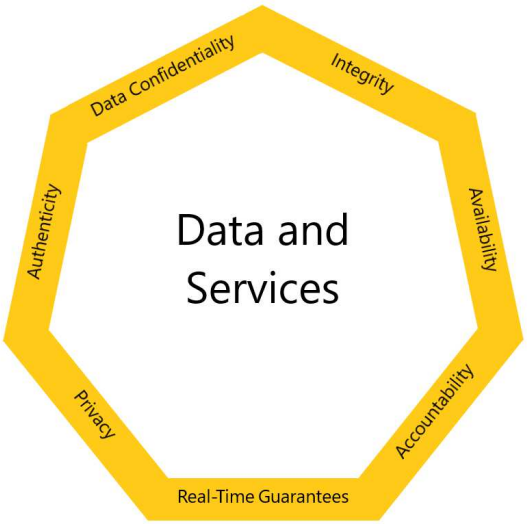


Figure 17: VANET Security Properties

5.1.1 Data Confidentiality

Data confidentiality is not essential for most VANET applications. Data confidentiality is only useful when certain ITS stations want to communicate privately. For example, in case a law enforcement vehicle wants to exchange sensitive data. [Pat11, p. 231]

In such cases, data confidentiality could be achieved by using encryption (e.g., as done with the ETSI C-ITS security header [Ins17d]).

5.1.2 Integrity

In VANETs, integrity could be partly provided by digital signatures or MACs. Digital signatures and MACs can ensure the integrity of hardware, software, data in transit, and data at rest within VANETs, as discussed in subsection 2.3.1 Data Confidentiality, Integrity, and Authenticity.

However, digital signatures cannot solve all integrity problems in VANETs (e.g., sensor tampering [Amo+15]). In particular, digital signatures cannot guarantee the correctness of content, as described in subsection 2.1.3 Further Security Properties. Information can be spoofed before sensors sense it [Cha16]. Though the sensed information would later be signed by a trustworthy ITS station, it would not be integer with respect to correctness of content, as described in subsection 2.1.1 Security Properties Triad.

For example, a sunlight sensor could be spoofed by pointing a source of light at it. Though the sensed information is technically correct, the information is not integer with respect to correctness of content.

To achieve correctness of content in VANETs, best-effort plausibility checks could be performed [Bis09, p. 41]. Extending the previous sunlight sensor example, it could, for example, be checked if the intensity of the sensed light could plausibly be the sun by checking the frequency spectrum of the light.

5.1.3 Availability

A lack of availability in VANETs may lead to traffic accidents [Qu+15]. As a result, availability is an important property in VANETs. Availability allows a VANET to remain operational in the presence of faults and attacks [Eng+14]. One important consideration for availability is resilience against DoS attacks [Bit17]. Such a resilience can be achieved by employing alternate means of communication, such as WiMax or 5G, by employing redundant infrastructure, and by using solutions that can scale with the size of potentially large VANETs [Bit17].

5.1.4 Authenticity, Accountability, and Privacy

In VANETs, authenticity, accountability, and privacy are closely related.

To prevent ITS station impersonation, authentication is necessary for messages in VANETs [Eng+14]. Apart from secure authentication of entities, authentication in VANETs has further requirements – entities must be able to communicate anonymously for privacy reasons, while authorized third-parties must be able to identify entities for liability and accountability reasons [Bit17]. The properties of privacy, as discussed in chapter 2 Fundamentals of IT Security, are realized by hiding the identity and/or the actions of a party from other participating parties. Accountability requirements are realized through information about the party's identity and actions [Pat11, pp. 231-234]. As these requirements conflict with each other, balancing them is a major challenge [Pat11, pp. 231-234]. It is, however, critical to find a good trade-off [Pat11, pp. 231-234]. To hold parties of VANETs accountable for their actions accountability is important [Pat11, pp. 231-234]. At the same time, vehicles are highly personal devices [Pat11, pp. 231-234]. Information about an individual's Smart Vehicle would allow an attacker to profile the individual rather accurately [Pat11, pp. 231-234].

Unlinkability can be achieved by using multiple short-lived pseudonyms (e.g., Raya and Hubaux [RH05]). With that, the unlinkability of a Smart Vehicle can be reset by changing its pseudonym [Bur+08]. However, Burmester et al. [Bur+08] argue that the purpose of short-lived pseudonyms can often be defeated by attackers that perform Bayesian traffic analysis. Most pseudonym change strategies can either be described as utilizing *hiding in the crowd* or *random silence* [Bur+08]. Burmester et al. [Bur+08] argue that unlinkability can only be upheld under Bayesian traffic analysis by strategies that utilize *hiding in the crowd* or both *hiding in the crowd* and *random silence*.

Schemes to provide unobservability in VANETs have not been widely discussed in current research.

Arguably, anonymity cannot be ensured in VANETs, as VANETs have accountability requirements that base on the identity of parties. Pseudonymity is a possible alternative to anonymity [PH10]. Pseudonymity prevents identification by other Smart Vehicles and allows accountability at the same time [PH10]. Pseudonymity can be achieved by using pseudonyms (e.g., Calandriello et al. [Cal+07]).

In current research, there are multiple pseudonym-based authentication schemes that provide accountability. Examples for such authentication schemes are the scheme by Calandriello et al. [Cal+07], the Pseudonymous Authentication-Based Conditional Privacy (PACP) protocol by Huang et al. [Hua+11], and the Authentication framework with A novel framework with Conditional Privacy-preservation and Non-repudiation (ACPN) by Li et al. [Li+14]. The scheme by Calandriello et al. is discussed later in this subsection.

Pseudonym-based authentication schemes often utilize pseudonym certificates (e.g., Calandriello et al. [Cal+07], Huang et al. [Hua+11], or Sun et al. [Sun+10]) [Li+14]. Pseudonym certificates are certificates that do not hold personal information themselves [Pet+14]. Instead, one or more infrastructure entities hold information that can link the certificates to a person [Pet+14]. This allows hiding the identity of one party from other participating parties [Pet+14]. At the same time, infrastructure entities can provide identities to authorized third-parties [Pet+14].

Calandriello et al. [Cal+07] present a scheme that provides efficient and robust pseudonym authentication in VANETs. The author's scheme is a combination of a pseudonym signature scheme and a group signature scheme. In the employed pseudonym scheme, a Smart Vehicle's long-term identity is held by a CA. The CA provides pseudonyms for the Smart Vehicle in the form of public-key certificates. These pseudonyms do not hold any information that can be used to identify the Smart Vehicle. In the employed group signature scheme, a Smart Vehicle belongs to a group, comprising of all Smart Vehicles registered with the CA, and is equipped with a secret per-vehicle group signing key and a group public key. These group keys enable group signatures. Group signatures allow any Smart Vehicle of a group to sign a message on the group's behalf without revealing its identity. It is also impossible to link any two signatures of a group member without a group manager's secret key. The possession of a group public key allows any entity to verify any group signature that was done with a corresponding group signing key.

In the scheme of Calandriello et al. [Cal+07], a Smart Vehicle first obtains a CA-provided pseudonym certificate. With this pseudonym certificate, the Smart Vehicle self-certifies a set of pseudonyms in the form of public-key certificates. Each self-certified pseudonym certificate is signed with a group signature. This self-certified pseudonym certificate is then used to sign messages. A verifier of such a message would first verify the group signature on the self-certified pseudonym certificate. The verifier would conclude that the pseudonym was created by a legitimate group member if the group signature verification was successful. Then, the verifier would verify the message content against the self-generated pseudonym certificate. If the verification is successful, the verifier can be sure that a Smart Vehicle with a certain pseudonym certificate belonging to a certain group has signed the message. However, the verifier cannot identify the Smart Vehicle belonging

to the pseudonym certificates or link any two different pseudonym certificates. In case it is required to identify a Smart Vehicle, authorized third-parties can request an *open* operation from the CA on a pseudonym certificate. Then, the CA would reveal the link between the self-certified pseudonym certificate, the CA-provided pseudonym certificate, and the identity corresponding to the CA-provided pseudonym certificate. [Cal+07]

5.2 Miscellanious Security Challenges of Vehicular Ad Hoc Networks

Other security challenges of VANETs, not attributable to particular security requirements, have been discussed by Yadav et al. [Yad+11] and Mokhtar and Azab [MA15]. These challenges are as follows.

5.2.1 Security Solutions in Short-Lived Topologies

Due to the short-lived topology of VANETs, most communication is between parties that have never interacted before and will likely not interact again soon after. Thus, security solutions that employ learning- or reputation-based schemes may have problems achieving good results. [Pat11, pp. 231-234]

In current research trust schemes, such as T-VNets by Kerrache et al. [Ker+16], REPLACE by Hu et al. [Hu+17], and the Attack-Resistant Trust (ART) management scheme by Li and Song [LS16] and misbehavior detection mechanisms, as discussed by van der Heijden et al. [Hei+18a], try to overcome detection problems in VANETs.

5.2.2 Scale of Network

Since VANETs are likely among the largest ad hoc networks in the near future, scalable solutions for availability and performance are required. Due to VANETs' size, pre-stored information about other participating parties or distribution of centralized information to all participating parties is not feasible. Instead, participating parties need to acquire information decentralized and on-demand, which makes it difficult to provide security. This is further exacerbated by the fact that security policies will differ from region to region. [Pat11, pp. 231-234]

5.2.3 Incentives for the Deployment of Security Solutions

For the effective deployment of VANETs it is necessary to provide incentives that lead all participating parties to adopt the system. As the participating parties can be diverse, various incentives will be required. Security further increases the cost and complexity of VANETs and therefore requires additional incentives. [Pat11, pp. 231-234]

5.2.4 Location Awareness

Most VANET applications require location-based services to be effective. This introduces reliance on the GNSS. Security flaws in GNSS likely reflect in VANET applications. [Pat11, pp. 231-234]

For example, GNSS is susceptible to GNSS spoofing. Various VANET applications that use GNSS have been shown to be susceptible to GNSS spoofing transitively. [Ham+15]

5.2.5 Real-Time Communication

Real-time communication is essential in VANETs, since road safety applications have a low critical latency. As a result, any implemented security mechanism needs to have a low processing and message overhead. [MA15]

In VANETs, major potentially performance-heavy security measures are cryptography and misbehavior detection. In current research, several authors discuss the performance of security measures in VANETs. Hamida et al. [Ham+15], Fernandes et al. [Fer+18], and Dai et al. [Dai+17] discuss the performance of cryptography for VANET usage. The performance of cryptography for VANET usage is discussed in more detail in section 9.5 Performant Cryptographic Algorithms for Vehicular Ad Hoc Networks. Arshad et al. [Ars+18] and Sakiz and Sen [SS17] discuss the performance of misbehavior detection. Misbehavior detection approaches for VANETs are described in section 9.6 Misbehavior Detection in Vehicular Ad Hoc Networks.

5.2.6 Multi-Hop Communication

VANETs frequently depend on multi-hop communication to send information to a target ITS station. This potentially allows intermediary parties to maliciously influence the sent information. Multi-hop communication mainly resides in the network protocol of a VANET and is a major attack vector for DoS attacks. [Eng+14]

5.3 Attacks on the Network Layer of Vehicular Ad Hoc Networks

In VANETs individual ITS stations are responsible for routing decisions. This makes it rather easy for misbehaving ITS stations to perform attacks. Network layer attacks have been studied extensively in the past years. The idea behind network layer attacks on VANETs is to absorb network traffic, inject yourself in the network traffic flow, and divert network traffic flow. [Pat11, p. 202]

There are various possible categorizations of network layer attacks with varying levels (e.g., Sakiz and Sen [SS17] or Pathan [Pat11, pp. 203-216]). The following categorization aims to have a minimal number of categories with only one sub-level. The listed attacks are partly inherited from MANETs [Pat11, p. 213]. These attacks are either widely

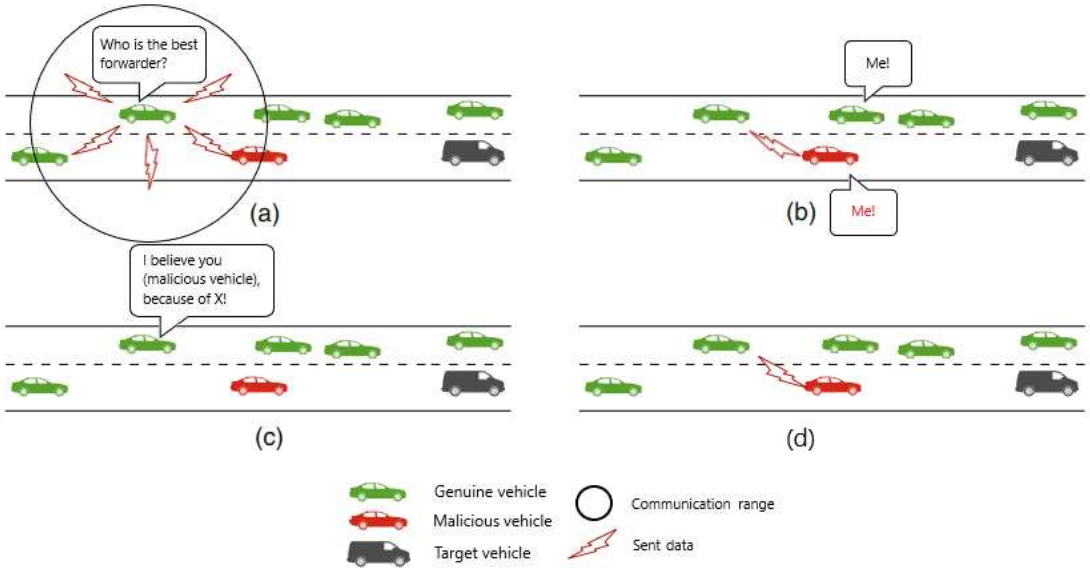


Figure 18: Sinkhole Attack: (a) Information Request by a Sender; (b) Response by the Neighboring Vehicles, One of which is Responding Maliciously; (c) The Sender Chooses the Malicious Vehicle as Forwarder of a Packet; (d) The Sender Sends the Packet to the Malicious Vehicle; (cf. [Men+18, pp. 32–34])

believed or have been shown to be applicable to VANETs (e.g., Shukla et al. [Shu+16], Hasrouny et al. [Has+17], Verma et al. [Ver+13], or Ponikwar and Hof [PH15]). However, the likelihood and the impact of the listed attacks on VANETs may differ from the impact on MANETs and depends on a VANET's exact security behavior. For example, the real-world impact of black hole attacks on MANETs differs from the real-world impact on VANETs, as discussed in subsection 6.1.1 Security-Relevant Properties.

The following categorization does not contain the category *black hole attacks* and its variant *gray hole attacks*. They are both described in more detail in the following chapter.

5.3.1 Sinkhole Attacks

In sinkhole attacks, an attacker tries to funnel traffic from a particular area through an ITS station they control [Ham+15]. This can be done by advertising the ITS station with properties that are desirable for the used routing protocols (e.g., by advertising the ITS station as the nearest ITS station to the destination). The attacker then controls the traffic and can perform further attacks, such as location disclosure attacks. [Ham+15]

Figure 18 shows a single sinkhole attack. Wormhole attacks and rushing attacks can be described as forms of sinkhole attacks.

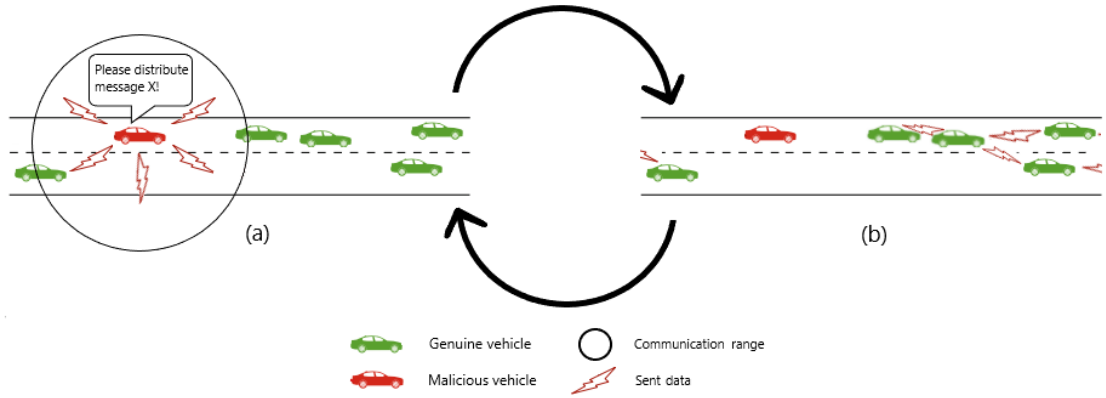


Figure 19: Flooding Attack: (a) A Malicious Vehicle Requests to Broadcast a Packet; (b) The Packet is Broadcasted; (cf. [Men+18, pp. 32–34])

5.3.2 Wormhole Attacks

In wormhole attacks an adversary links to otherwise distant regions of the network [Cha16]. This appears beneficial at first sight, since it improves network performance [Cha16]. However, this gives the adversary complete control of all traffic using the link [MA15]. Wormhole attacks are network layer attacks with severe impact on the underlying network. [Pat11, p. 205]

5.3.3 Rushing Attacks

In rushing attacks a malicious ITS station quickly forwards messages. Since an ITS station may only consider the fastest response to a request and discard later ones, a fast malicious ITS station may be able to include itself in a given route. [Pat11, p. 206]

5.3.4 Flooding Attacks

Flooding attacks aim to consume network resources to degrade the network's or the ITS station's performance [Ham+15]. There are two common types of such attacks: route request flooding attacks and data flooding attacks [Pat11, pp. 204-205]. Depending on the exact attack scenario, such attacks may be prevented or mitigated by flood management mechanisms. [Pat11, pp. 204-205]

Flooding attacks can be performed by executing a single network resource-heavy task numerous times in quick succession (e.g., Desilva and Boppana [DB05]). Figure 19 displays a repeated network resource-heavy task.

Desilva and Boppana [DB05] have shown that route request flooding attacks, a certain type of flooding attacks, can lead to performance degradation of up to 84%.

5.3.5 Link-Withholding Attacks

In link-withholding attacks, an attacker withholds a route or ignores the requirement to advertise a route between two or more ITS stations. Thus, these ITS stations may be unable to find links to communicate with each other, leading to a DoS. [Pat11, p. 206]

5.3.6 Link-Spoofing Attacks

In link-spoofing attacks, an attacker forges a route between two or more ITS stations. This may lead the source ITS station to choose the malicious ITS station as a forwarder, allowing it to perform attacks, such as location disclosure attacks. [Pat11, p. 206]

5.3.7 Byzantine Attacks

In byzantine attacks, multiple malicious ITS stations collude to perform attacks, such as routing loops or non-optimal path selection. This leads to a degradation or disruption of the network. One subtype of such attacks are colluding misrelay attacks. [Pat11, p. 206]

5.3.8 Colluding Misrelay Attacks

In colluding misrelay attacks multiple malicious ITS stations collude to modify or drop routing packets to disrupt routing operations. [Pat11, p. 204]

5.3.9 Replay Attacks

In replay attacks, a malicious ITS station records a victim ITS station's packets and resends them later. This might allow an attacker to impersonate the victim ITS station or to disturb the routing operation of a network by introducing stale routes. [Pat11, p. 204]

Figure 20 shows a successful replay attack.

5.3.10 Location Disclosure Attacks

In location disclosure attacks, an attacker finds out location information of ITS stations or the structure of a network. With that, the attacker can plan further attack scenarios. This attack gives away the anonymity required in VANETs. [Pat11, p. 204]

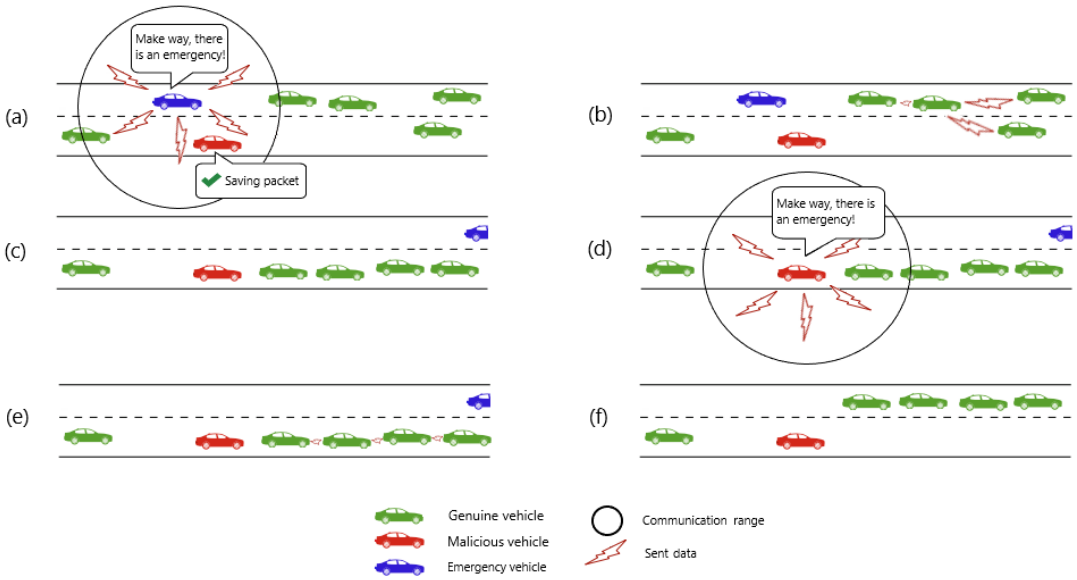


Figure 20: Replay Attack: (a) An Emergency Vehicle sends a Request to Make Way and a Malicious Vehicle Saves the Corresponding Packet; (b) The Packet is Distributed; (c) The Vehicles Make Way for the Emergency Vehicle; (d) The Malicious Vehicle Replays the Packet; (e) The Replayed Packet is Distributed; (f) The Vehicles Make Way for the Malicious Vehicle; (cf. [Men+18, pp. 32–34])

CHAPTER 6

Black Hole Attacks in Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks

This chapter describes black hole attacks in MANETs and VANETs. For that, a definition of black hole attacks in MANETs is provided. Then security-relevant properties of black hole attacks on MANETs are discussed. Later, gray hole attacks, a variant of black hole attacks, are explained.

The definition of black hole attacks and the security-relevant properties of VANETs are then (partly) inferred from MANETs.

This chapter uses the terminology for the description of information dissemination paradigms that is given in subsection 4.3.2 GeoNetworking.

6.1 Black Hole Attacks in Mobile Ad Hoc Networks

In current research black hole attacks are described in varying manners (e.g., Tseng et al. [Tse+18], Jaydip [Jay11], or Tamilselvan and Sankaranarayanan [TS07; TS08]).

Jaydip [Jay11] describes a black hole attack as an attack in which a malicious node exploits the routing protocol to advertise itself as having a valid route to a destination, with the intention of intercepting packets. Because of the malicious node's advertising, the malicious node is selected for routing and receives the packets. Instead of forwarding the packets, the malicious node drops the packets. This description (1) does not consider *cooperative* black hole attacks, as described by Tamilselvan and Sankaranarayanan [TS08], and also does not consider that (2) it is not sufficient for an attacker to advertise themselves to have *a valid route* to a destination to get selected for routing. To address flaw (1), it must be considered that multiple cooperative malicious nodes can perform a

black hole attack [TS08]. To address flaw (2), it must be considered that the underlying routing protocol may consider multiple potential forwarders for routing (e.g., GF, as described in subsection 4.3.1 Network Layer), so that having *a valid route* makes the malicious node only a potential forwarder. Rather, to get selected for routing by the underlying routing protocol an attacker would have to have the optimal route to a destination according to the routing protocol.

Tamilselvan and Sankaranarayanan [TS07; TS08] describe black hole attack as a DoS attack in which one malicious node or multiple cooperative malicious nodes can attract all packets by falsely claiming to have a route to a destination and then drop all packets. Analogously to the description by Pathan, the description by Tamilselvan and Sankaranarayanan does not consider that claiming to have *a route* to a destination is not sufficient to absorb packets. One malicious node or multiple malicious nodes would have to claim to have the best route to a destination for all packets. Furthermore, the description by Tamilselvan and Sankaranarayanan considers *all packets* without limiting the scope in which *all packets* has to be understood. A reader of the description could think all packets of a whole VANET are meant. To address this imprecision, a scope must be defined.

Tseng et al. [Tse+18] describe black hole attacks as attacks where one or more malicious nodes violate routing rules by varying means and drop all received packets. Arguably, the formulation of the violation of routing rules is vague and does not consider any absorption of traffic or advertising/claiming to even have a route. As a result of the vague formulation, this formulation of black hole attacks cannot be considered precise.

With the aim to be more complete and more precise than the descriptions of Jaydip [Jay11], of Tamilselvan and Sankaranarayanan [TS07; TS08], and of Tseng et al. [Tse+18], this thesis employs its own definition of black hole attacks. This definition is as follows:

> A black hole attack is defined as an attack where one malicious or multiple cooperative malicious nodes
>
> (1) advertise themselves to have an optimal route to a destination for all packets in their communication range in order to absorb the packets and
>
> (2) drop the packets in a way that the packets do not reach their destination.

Phase (1) can be described as absorbing all packets in the communication range of the attacker(s). Phase (2) can simply be described as dropping all these packets.

In the Border Gateway Protocol (BGP), there is a concept similar to black hole attacks: blackholing. This concept is described in section 9.3 Blackholing in the Border Gateway Protocol.

Research related to MANETs is discussed in section 9.4 Mobile Ad Hoc Networks.

6.1.1 Security-Relevant Properties

In this subsection, MANET properties that are relevant for the security against black hole attacks are identified. These security-relevant properties influence the impact and/or likelihood of black hole attacks on MANETs. It should be noted that the provided enumeration of security-relevant properties is non-exhaustive.

Forwarder Selection of the Employed Routing Protocol

Glass et al. [Gla+11] classifies black hole attacks as attacks against packet forwarding. This indicates that the forwarding mechanism, or more specifically the forwarder selection, is a security-relevant property for black hole attacks on MANETs.

In this chapter, the forwarder selection is described based on two categories: forwarder selection at the sender and forwarder selection at the intermediary recipient. From a security perspective, the location of the forwarder selection is important because, depending on the location, an attacker has different capabilities and options to exploit the forwarder selection. These capabilities and options are described in the following of this subsubsection.

In routing protocols that perform forwarder selection at the sender, the sender will perform a pre-selection of the next intermediary recipient. In such cases, an attacker can perform phase (1) of a black hole attack by forging data, so that the attacker is the optimal intermediary recipient. This, in turn, allows the attacker to perform phase (2) of a black hole attack. An example of a routing protocol in which the forwarding algorithm performs forwarder selection at the sender is OLSR [Cla+03].

In routing protocols that perform forwarder selection at the intermediary recipient, the forwarding node would broadcast the packet in question to all nodes in range. One or more of the nodes which received the packet then forward the packet. In such cases, an attacker would have to convince other nodes that received the packet to refrain from forwarding it. An example of a routing protocol that performs forwarder selection at the intermediary recipient is CBF [Füß+03].

Robustness of the Employed Routing Protocol

The impact of black hole attacks on a routing protocol arguably significantly depends on the robustness of the routing protocol. A routing protocol that is not robust against black hole attacks will be highly impacted by a black hole attack, while a routing protocol that is robust to black hole attacks will suffer a lower impact. Well-known MANET routing protocols, such as AODV or OLSR, have a different robustness against black hole attacks (e.g., Bala et al. [Bal+09], Esmaili et al. [Esm+11], or Ulla and Rehman [UR10]). Though the differences in robustness can be analyzed theoretically (e.g., Tamilselvan and Sankaranarayan [TS07; TS08]), they can be assessed more practically through performance analyses (e.g., Bala et al. [Bal+09], Esmaili et al. [Esm+11], or Ulla and Rehman [UR10]).

In current research high-quality performance analyses for these protocols are sparse. Only research for AODV and OLSR is of sufficient quality for this thesis. Relatively good quality performance analyses for AODV and OLSR have been done by Bala et al. [Bal+09], Esmaili et al. [Esm+11], and Ulla and Rehman [UR10]. The performance analysis of Ulla and Rehman seems to have been plagiarized by Bibhu et al. [Bib+12]. The figures in the work of Bibhu et al. are clearly exact copies of the figures in the work of Ulla and Rehman.

In the following of this subsubsection, the performance analyses of Bala et al. [Bal+09], Esmaili et al. [Esm+11], and Ulla and Rehman [UR10] are described. For the definition of performance metrics, it is referred to the respective article.

Bala et al. [Bal+09] analyze the performance impact of black hole attacks on AODV. The simulation is conducted over a timespan of 500s with 20 nodes, 0 to 1 black hole attackers, and speeds varying between 10km/h and 50km/h. The simulation shows a packet loss of up to 89.38% in the presence of an attacker, while the maximum packet loss was only 2.50% in the absence of an attacker. The throughput suffered a similarly negative impact. The average end-to-end delay is slightly lower in the presence of an attacker. This decrease in end-to-end delay can be explained by the immediate reply a malicious node gives, as the malicious node does not have to check its routing table. The authors further show an increasing impact on the throughput when the number of black hole attackers increases to 4. Arguably, the impact on packet loss and throughput of even one black hole attacker would be devastating to the MANET. The devastating impact for such a low number of black hole attackers makes the results seem very unrealistic.

Esmaili et al. [Esm+11] found a lower impact of black hole attacks on AODV in a simulation scenario over 600s with 46 nodes, 0 to 4 black hole attackers, and speeds varying between 0km/h and 108km/h. The simulation shows a reduction of the packet delivery ratio of 85.78% in the absence of a black hole attacker to 35.25% in the presence of one attacker. The packet delivery ratio further decreases down to 21.79% in the presence of up to four attackers. Notably, the lower impact of this analysis compared to the analysis of Bala et al. may be explained, to some extent, by a higher sample size and/or a lower attacker/node ratio.

Ulla and Rehman [UR10] conducted a performance analysis of AODV and OLSR. It was found that AODV is more affected by black hole attacks than OLSR regarding most network performance metrics. The simulation was performed with 16 and 30 nodes and 0 to 1 black hole attacker over 1000 seconds. The nodes moved based on a random way path model with a constant speed of 10m/s. For simplicity, only the results with 30 nodes at the end of the simulation time are discussed here. As the authors did not publish detailed numbers of the results, the deltas of the performance metrics between 0 and 1 black hole attackers are extrapolated from figures in the paper. For end-to-end delay, AODV shows a decrease of roughly 22%. OLSR showed no significant decrease in end-to-end delay. In OLSR, throughput decreases by about 10%. This is similar to the approximately 10% decrease in throughput in AODV. Regarding the network load, AODV shows no significant change, while OLSR has a decrease of about 30%.

Security Mechanism of the Employed Routing Protocol

The security mechanism of the employed routing protocol is a security-relevant property. A security mechanism can ensure the accuracy of the information on which the routing protocol bases (e.g., Tamilselvan and Sankaranarayan [TS07]). Furthermore, a security mechanism can allow to detect misbehaving senders/recipients/forwarders and remove them from the routing process (e.g., Tamilselvan and Sankaranarayanan [TS08]).

Tamilselvan and Sankaranarayan [TS07] and Ramaswamy et al. [Ram+03] have both extended the well-known reactive routing protocol AODV independently to overcome black hole attacks. Both extensions employ a security mechanism that shall ensure the accuracy of routing information. Notably, the security mechanism proposed by Tamilselvan and Sankaranarayan only prevents non-cooperative black hole attacks, while the security mechanism proposed by Ramaswamy et al. prevents cooperative black hole attacks. To prevent cooperative black hole attacks, Tamilselvan and Sankaranarayanan [TS08] have developed another security mechanism for AODV. The security mechanisms by Ramaswamy et al. and by Tamilselvan and Sankaranarayanan essentially employ a misbehavior detection and exclude misbehaving nodes from the routing process.

Attacker/Node Ratio and Cooperativeness

Intuitivel,y and shown by the performance analysis of Esmaili et al. [Esm+11], the attacker/node ratio significantly influences the impact of a black hole attack. From this performance analysis it can be inferred that a MANET performs worse with an increasing attacker/node ratio. The impact of a black hole attack is further influenced by the cooperativeness of the attackers, as discussed by Tamilselvan and Sankaranarayanan [TS08]. Depending on the robustness of the routing protocol and its security mechanisms the attacker/node ratio and their cooperativeness may even influence the likelihood of a black hole attack. Cooperatively working attackers may be able to circumvent security mechanisms in routing protocols that only prevent non-cooperative black hole attacks, such as the security mechanism of Tamilselvan and Sankaranarayan [TS07].

Node Speed and Attacker Proxmity

The performance analysis of Tamilselvan and Sankaranarayanan [TS07] shows that the nodes' speeds and attacker proximity do not only significantly influence the overall performance of a routing protocol, but can also significantly influence the impact of a black hole attack. For AODV, the authors found that, depending on the speed and the proximity of the attacker to the source node, the packet delivery ratio differs significantly. In the absence of a black hole attacker and neglecting nodes' speeds of 0m/s, AODV has a packet delivery ratio of between ~67% and 90% for speeds between 10 and 80m/s. In the presence of a black hole attacker in close proximity to the source node, AODV's packet delivery ratio lies between ~5% and 30%. In the presence of a black hole attacker who is not in close proximity to the source node, AODV's packet delivery ratio is between

~25% and ~80%. In AODV end-to-end delay does not differ significantly regardless of the nodes' speed and attacker proximity.

Safety-Criticality of the Mobile Ad Hoc Network

Aside VANETs, a well-known manifestation of MANETs is the iMANET [RD13]. As exemplified in the following of this subsubsection, the real-world impact of black hole attacks is influenced by the safety-criticality of the particular use case of a MANET.

IMANETs have several use cases, such as military use cases, law enforcement uses cases, or educational use cases [Kal+13]. Arguably, the real-world impact of black hole attacks in an iMANET used for military purposes or law enforcement purposes is much higher than for education purposes. In military surveillance, for example, packets lost due to a black hole attack may frequently contain information that is critical to save the lives of individuals or groups. On the other hand, in education, packets lost due to a black hole attack do not endanger human life.

6.1.2 Gray Hole Attacks

Black hole attacks have one variant: gray hole attacks. In gray hole attacks, instead of dropping packets altogether, a malicious node or multiple malicious nodes only selectively drop packets (e.g., packets of a certain type). Due to the selective misbehavior of malicious nodes, gray hole attacks are rather difficult to detect. [Cha16]

6.2 Black Hole Attacks in Vehicular Ad Hoc Networks

In this thesis, black hole attacks in VANETs follow the same definition as black hole attacks in MANETs. The process of performing phase (1) and phase (2) of a black hole attack on a single packet in a VANET is displayed in Figure 21. If this process was done for all packets in the communication range of one or multiple attackers, the attack would constitute a black hole attack.

As stated in section 5.1 Security Requirements and Related Challenges VANETs inherit many security characteristics from MANETs. It is argued that VANETs inherit the previously identified security-relevant properties from MANETs, as done with many other characteristics and properties of MANETs (e.g. Grover et al. [Gro+11], Meneguette et al. [Men+18, pp. 28-29], Qu et al. [Qu+15], Bittl [Bit17]). In the following subsection, the security-relevant property *robustness of the employed routing protocol* is discussed for well-known VANET routing protocols

6.2.1 Robustness of Well-Known Vehicular Ad Hoc Network Routing Protocols

The discussion in this subsection aims to identify the robustness of well-known VANET routing protocols against black hole attacks.

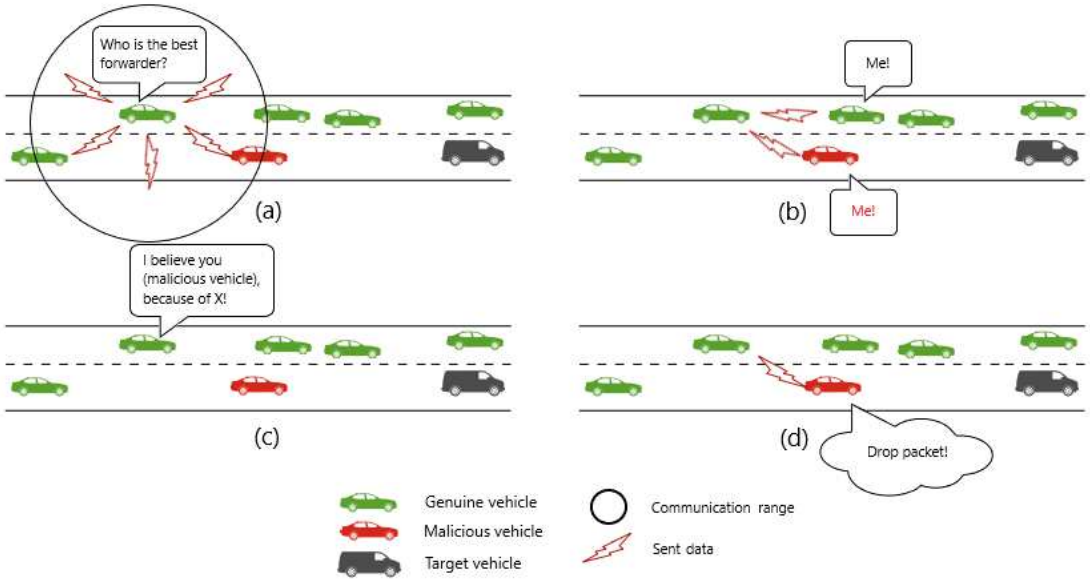


Figure 21: Phase (1) and Phase (2) of a Black Hole Attack on a Single Packet in a VANET: (a) Information Request by a Sender; (b) Response by the Neighboring Vehicles, One of which is Responding Maliciously; (c) The Sender Chooses the Malicious Vehicle as Forwarder of a Packet; (d) The Sender Sends the Packet to the Malicious Vehicle and the Malicious Vehicle Drops the Packet; (cf. [Men+18, pp. 32–34])

Realistic Traffic Scenarios in Vehicular Ad Hoc Network Simulations

MANET routing protocols are often used in VANET research (e.g., Dixit et al. [Dix+16], Saeed et al. [Sae+12], Singh and Agrawal [SA14], or Paul et al. [Pau+12]). However, performance analyses of MANET routing protocols under black hole attacks cannot be used unequivocally to infer the performance of the same routing protocols under black hole attacks in VANETs [MS15, pp. 312-313]. That is because nodes in MANETs behave differently than Smart Vehicles in VANETs [MS15]. While nodes in MANETs do not have typical movement patterns, Smart Vehicles drive along various road topologies (e.g., intersections, country roads, etc.) with varying Smart Vehicle density and in speeds typical for the area the Smart Vehicles are in [MS15, pp. 312-313]. Research in VANETs frequently considers three different areas: urban areas, highways, and rural areas [Ins12a].

To accurately measure the robustness of routing protocols, only performance analyses that realistically reflect real-world traffic scenarios are discussed here. In this thesis, a traffic scenario is considered realistic if

- the road topology that Smart Vehicles drive on is representative for at least one small-scale subscenario of either an urban area, a highway, or a rural area.

Examples for subscenarios in urban areas, highways, and rural areas are frequented intersections with traffic lights, high-density traffic on highway-shaped roads, and low-density traffic on typical country roads respectively,

- the traffic scenario employs Smart Vehicles that drive at a speed that is plausible in the respective traffic scenario, i.e., speeds of approximately 0 to 50 km/h in urban areas, speeds of approximately 0 to 100 km/h in rural areas, and speeds of over 100 km/h on highways,
- and the traffic scenario has a meaningful number of Smart Vehicles for the respective traffic scenario.

Without providing proof, it is argued that using a realistic traffic scenario for VANET simulations inherently leads to simulations with relatively high realism. This assumption is based on the presumption that traffic scenarios are a central element of VANET simulations, as indicated by Riebl et al. [Rie+19] and Lin and Lu [LL15, pp. 41-42].

Methodology for Deducting the Robustness of Routing Protocols

As the following discussion aims to measure the robustness of routing protocols against black hole attacks, not all methodologies to conduct performance analyses are suitable for this thesis. To be able to deduct the robustness of routing protocols, simulations in the performance analyses are required to be conducted and documented in the absence of black hole attackers and the presence of one or more black hole attackers. The conduction and documentation of such a simulation allow to directly compare the performance of a scenario in the absence of black hole attackers with the performance of a scenario in the presence of one or more black hole attackers on each tested routing protocol. This comparison allows to deduct the performance impact of one or more black hole attackers.

Analysis of Performance Analyses in Current Research

The criteria for realistic traffic scenarios and the criteria for methodology are only met by the performance analysis of Grimaldo and Martí [GM18]. This performance analysis is discussed later in this subsubsection. Many other performance analyses are not suitable for this thesis. These unsuitable performance analyses employ non-realistic traffic scenarios that use random waypoint mobility with constant speed (e.g., Ahmed et al. [Ahm+14] or Bibhu et al. [Bib+12]), do not conduct and document simulations in the absence of black hole attackers and the presence of one or more black hole attackers (e.g., Tyagi and Dembla [TD17], Hamid and Mokhtar [HM15], Purohit et al. [Pur+17], or Lachdhaf et al. [Lac+17]), do not specify the employed traffic scenario at all (e.g., Kumar et al. [KS19]), or exhibit an implausible traffic scenario (e.g., Afdhal et al. [Afd+17]). The performance analysis of Afdhal et al. uses a two-lane road topology of 1000m with 10 Smart Vehicles driving at random speeds between 40km/h and 80km/h. The simulation time is 100 seconds. Even if all Smart Vehicles were driving at the slowest speed of

Protocol Name	Packet Delivery Ratio	Network Overhead	End-To-End Delay
AODV with One Black Hole Attacker	approx. -5%	approx. -3% to -20%	approx. -3% to -20%
DSR with One Black Hole Attacker	approx. -20%	approx. -0%	approx. -0%
OLSR with One Black Hole Attacker	approx. -5%	approx. -0% to -5%	approx. -0%
DSDV with One Black Hole Attacker	approx. -5%	approx. -0%	approx. -0%

Table 5: Impact of Black Hole Attacks on AODV, DSR, OLSR, and DSDV in an Urban Traffic Scenario [GM18]

40km/h, they would reach the end of the road before the simulation ends. As Afdhal et al. do not provide more detailed information about the traffic scenario, it is unclear if the Smart Vehicles would either continue driving with their assigned speed, essentially leaving the road topology or suddenly stop driving, aggregating at the end of the simulation area. Arguably, in any plausible traffic scenario, neither of the two cases could happen.

Grimaldo and Martí [GM18] performed an analysis of AODV, DSR, OLSR, and DSDV. A simulation was performed over 300 seconds with a 1.5km x 1.5km road topology excerpt from Panama City. This road topology includes multiple intersections and one-way streets as well as bidirectional two-lane streets. The simulation employed 80 Smart Vehicles of which 0 to 1 were a black hole attacker. To ensure realistic vehicle speeds, the authors factored speed limits and additionally employed the Krauss model by Krauss et al. [Kra+97], which chooses a safe speed based on traffic and road topology (e.g., intersections or traffic lights). The results of the simulation are summarized in Table 5. This table shows the decrease of packet delivery ratio, network overhead, and end-to-end delay in the presence of a black hole attacker compared to the absence of a black hole attacker. It appears that there is a ramp-up time in the simulation of about 50 seconds. As a result, only data after 50 seconds is considered for the comparison here. As the authors do not provide exact data for network overhead and end-to-end delay, this data is extrapolated from the figures of Grimaldo and Martí [GM18]. AODV shows a relatively high increase in end-to-end delay and network overhead and a slight decrease in packet delivery ratio. DSDV and OLSR are only minorly impacted by black hole attacks. The packet delivery ratio of DSR is strongly impacted relative to the other analyzed protocols.

As the results of Grimaldo and Martí [GM18] are the first of their kind in an urban traffic scenario, these results have yet to be confirmed in further performance analyses.

CHAPTER 7

Security of the GeoNetworking Protocol against Black Hole Attacks

In this chapter, the security of the GeoNetworking protocol against black hole attacks is analyzed. For that, the security-relevant property *robustness of the employed routing protocol*, as defined in subsection 6.1.1 Security-Relevant Properties and analyzed for well-known VANET routing protocols in subsection 6.2.1 Robustness of Well-Known Vehicular Ad Hoc Network Routing Protocols, is assessed for the GeoNetworking protocol. Then, the risk of black hole attacks in ETSI C-ITS, as it had been identified in a risk analysis in ETSI TR 102 893 [Ins17b] is briefly discussed. The discussion of the risk analysis in ETSI TR 102 893 is followed by a description of security measures against black hole attacks on ETSI C-ITS.

Based on the robustness analysis conducted earlier in this chapter, a risk analysis is conducted using the methodology of ETSI TS 102 165-1 version 4.2.3 [Ins11a]. In contrast to the risk analysis in ETSI TR 102 893 [Ins17b], the risk analysis performed in this chapter differentiates the risk of black hole attacks individually on each forwarding algorithm. The risk analysis in this chapter is divided into a risk analysis without security measures and risk analyses with different ETSI C-ITS security measures.

7.1 Robustness of the GeoNetworking Protocol

As described in subsection 4.3.1 Network Layer, the Geonetworking protocol consists of several forwarding algorithms some of which function fundamentally differently. This different functionality potentially leads to different security behavior of the forwarding algorithms. For example, GF has no mechanism to deal with communication failures, while CBF has a mechanism to deal with communication failures [Ins11b]. As a black

hole attack could be considered a communication failure, this mechanism in CBF may lead to CBF being more robust against black hole attacks than GF.

As a result of the potentially different security behavior of the forwarding algorithms of the GeoNetworking protocol, the robustness of the GeoNetworking protocol in the following of this section is analyzed for each forwarding algorithm of the GeoNetworking protocol individually. Notably, only fully standardized forwarding algorithms are considered in the following of this section.

7.1.1 N-Hop Broadcast Forwarding in Topologically Scoped Broadcast

Following the definition of black hole attacks given in section 6.1 Black Hole Attacks in Mobile Ad Hoc Networks, in phase (1) of a black hole attack all NHBF packets must be absorbed. In NHBF, there is no advertising functionality or optimal forwarder selection that would allow an ITS station to absorb packets. As described in subsection 4.3.1 Network Layer, any ITS station that receives an NHBF packet simply forwards the packet until it reaches its maximum hop count. As an absorption of NHBF packets is not possible, phase (1) of a black hole attack cannot be performed. As a result, black hole attacks on NHBF are not possible.

7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding

GF packets, as used in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding, are vulnerable to black hole attacks. In the followingly described attack scenario, it is explained how a malicious ITS station could successfully perform phase (1) and phase (2) of a black hole attack for a single GF packet. Then, it is described how phase (1) and phase (2) can be conducted for all GF packets.

As described in subsection 4.3.1 Network Layer, in GF, a sender selects the neighbor with the smallest geographic distance to the destination from their location table as the optimal forwarder. This location table is filled by periodically sent beacons. As the authenticity of beacons is not checked, without any further security measures, data in these beacons can be set arbitrarily. This means a malicious ITS station can fake data in the beacons, for example, the sending ITS station's logical link address, the sending ITS station's GeoNetworking address, or the sending ITS station's location. A recipient of a beacon would be unable to detect such faked information.

To perform phase (1) of a black hole attack on a single packet, a malicious ITS station can make a sender believe that they have the smallest geographic distance to the destination by sending a beacon with a faked logical link address, a faked GeoNetworking address, and a faked location. This faked location would be slightly outside the communication range of the sender and thus, farther away than any other genuine potential forwarder. As a result, a sender will choose the ITS station that faked its location information as

an optimal forwarder when sending packets in the direction of the faked location. An example of this process is displayed in Figure 22. In this example, it can be seen that faking locations in such a manner can absorb packets that are targeted in the direction of the faked location. To absorb a packet regardless of the direction it is headed, a malicious ITS station could send multiple beacons with a faked logical link address, a faked GeoNetworking address, and a faked location (i.e., effectively spoofing an ITS station) in a circle-like shape, as displayed in Figure 23. Each spoofed ITS station would be farther away than any other genuine potential intermediary recipient in the communication range of the sender. As a result, a sender will, regardless of a packet's transmission direction, always choose a spoofed ITS station as the optimal forwarder. As the logical link addresses and the GeoNetworking addresses of all spoofed ITS stations are fake, the transmitted packets are not processed by any actual ITS station. To perform phase (2) of a black hole attack on a single packet, no action has to be taken. The underlying problem of this scenario could be described in the following way: Senders are unable to check the authenticity of location table information which allows an attacker to spoof ITS station.

Instead of performing phase (1) and phase (2) of a black hole attack on only a single packet, a malicious ITS station could perform both phases on all GF packets.

7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast

Theoretically, CBF packets, as used by GeoUnicast and GeoAnycast, can be attacked with black hole attacks. In the followingly described attack scenario, it is explained how a malicious ITS station could successfully perform phase (1) and phase (2) of a black hole attack for a single CBF packet. Then, it is described how phase (1) and phase (2) can be conducted for all CBF packets.

As described in subsection 4.3.1 Network Layer, in CBF, the intermediary recipient that first rebroadcasts the packet is considered the optimal forwarder of a packet. All other intermediary recipients then refrain from forwarding the packet. By making every genuine intermediary recipient believe that the packet has been rebroadcasted, a malicious ITS station can perform phase (1) and phase (2) of a black hole attack simultaneously on a single packet. Such a trickery could be achieved by identifying every ITS station that has an active retransmission timer for the packet in question through a physical simulation of the packet transmission that started the retransmission timer. The therewith identified ITS stations can be targeted through one or more highly precise directional antennas. With these directional antennas, one or multiple malicious ITS stations would retransmit the packet to any ITS station with an active retransmission timer for the packet. This retransmission would make genuine intermediary recipients believe that the packet has been rebroadcasted, despite it only being resent to ITS stations with an active retransmission timer for that packet and not to other ITS stations. The underlying problem of this scenario could be described in the following way: Intermediary recipients with an active retransmission timer for a packet cannot easily check if an ITS station only retransmitted the CBF packet to them in a targeted manner or actually rebroadcasted

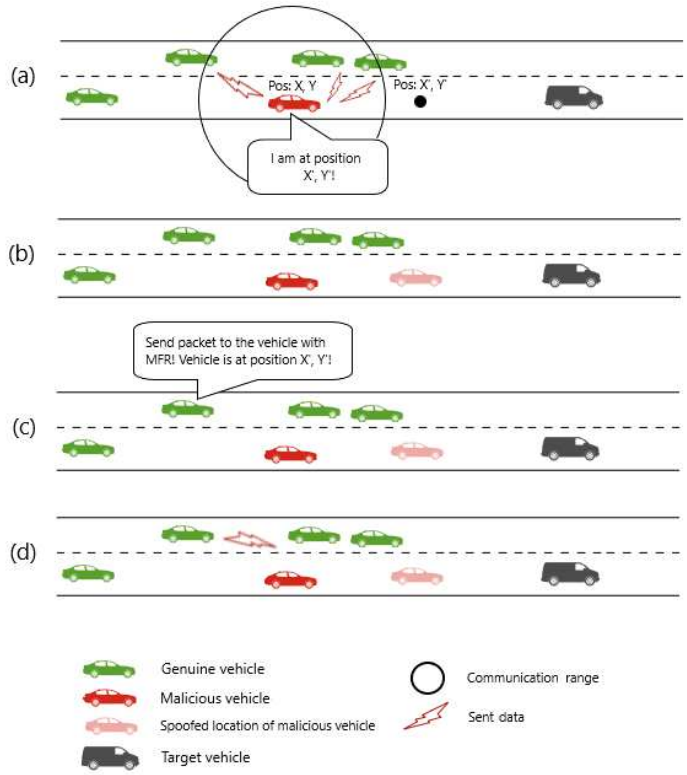


Figure 22: Phase (1) and Phase (2) of a Black Hole Attack on a Single GF Packet Sent in a Specific Direction: (a) A Malicious Vehicle Sends a Beacon with a Spoofed Location; (b) All Vehicles that Received the Beacon Believe there is a Vehicle at the Spoofed Location; (c) A Sender Sends a GF Packet to the Vehicle with the MFR, which Is the Spoofed Vehicle; (d) The Spoofed Vehicle Does not Exist, so the Packet is Effectively Dropped; (cf. [Men+18, pp. 32–34])

the packet. For the scenario to be successful, a malicious ITS station must ignore its retransmission timer. The whole scenario is exemplified in Figure 24. It remains to be shown that such a scenario is feasible in practice. Various physical effects may render precisely targeting certain ITS stations infeasible.

Instead of performing phase (1) and phase (2) of a black hole attack on only a single packet, a malicious ITS station could perform both phases on all CBF packets.

7.1.4 GeoBroadcast Forwarding in Simple GeoBroadcast Forwarding

Analogously to NHBF, GBF, as used in Simple GeoBroadcast Forwarding, does not employ any advertising functionality or optimal forwarder selection. As described in subsection 4.3.1 Network Layer, any ITS station that receives a GBF packet simply

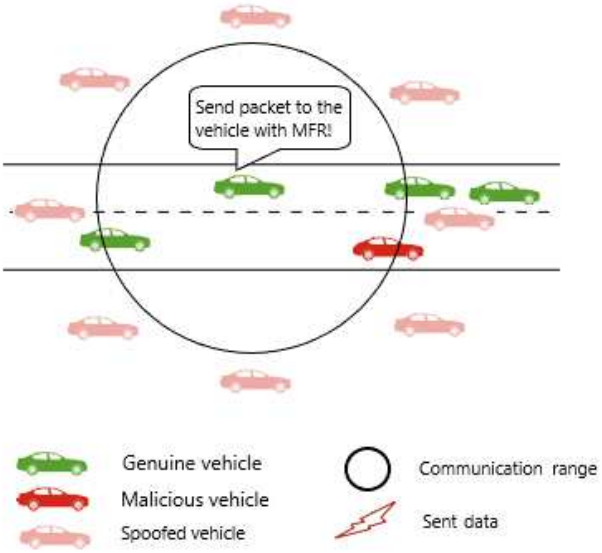


Figure 23: Phase (1) and Phase (2) of a Black Hole Attack on a Single GF Packet Sent in any Direction (cf. [Men+18, pp. 32–34])

rebroadcasts the packet if the ITS station is within the geographic target area of the packet. As a result, black hole attacks cannot be performed on GBF.

7.2 Methodology in the ETSI Technical Specification 102 165-1 Version 4.2.3

The risk analysis in ETSI TR 102 893 [Ins17b] and the risk analysis later in this thesis follow the methodology described in ETSI TS 102 165-1 version 4.2.3 [Ins11a]. This methodology is described in the following of this section.

7.2.1 Attack Factors

ETSI TS 102 165-1 version 4.2.3 [Ins11a] categorizes possible opportunity levels as follows:

- **Unnecessary/unlimited access** – an attack does not need any kind of opportunity to be realized. [Ins11a]
- **Easy** – an attack takes less than a day or the number of asset samples required to perform the attack is less than ten. [Ins11a]
- **Moderate** – an attack takes less than a month or the number of asset samples required to perform the attack is less than fifty. [Ins11a]

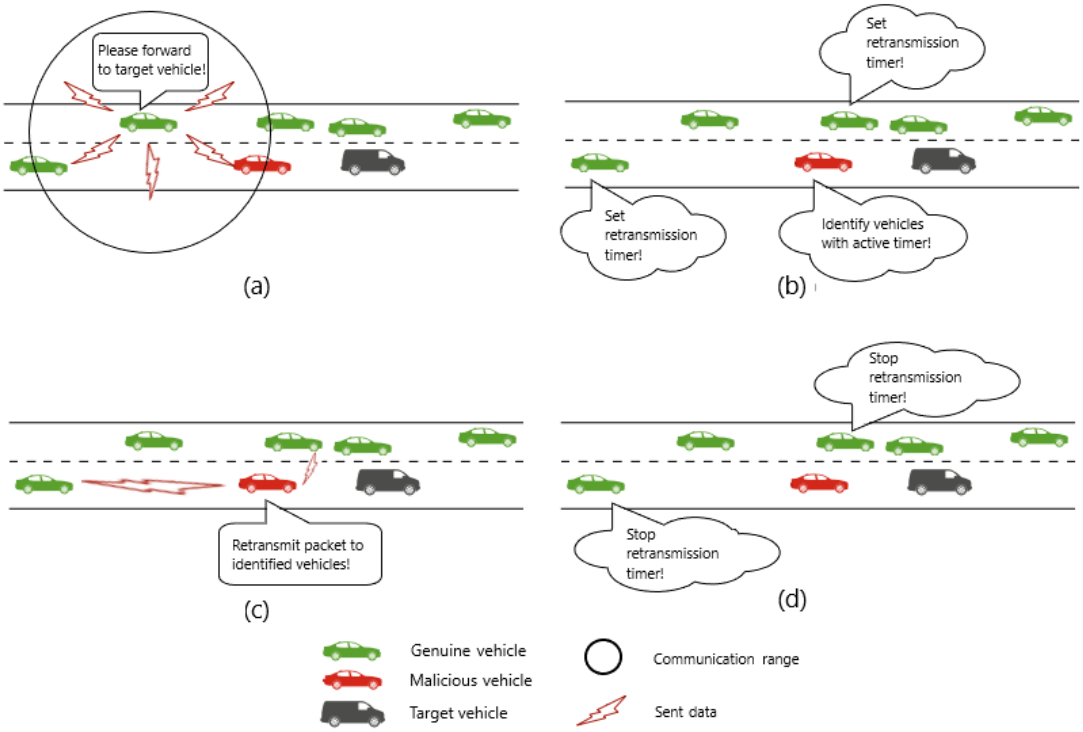


Figure 24: Phase (1) and Phase (2) of a Black Hole Attack on a Single CBF Packet: (a) A Sender Sends a Packet; (b) The Receiving Vehicles set Their Retransmission Timers and the the Malicious Vehicle Identifies all Vehicles with an Active Retransmission Timer; (c) The Malicious Vehicle Retransmits the Packet to the Identified Vehicles; (d) The Vehicles Stop Their Retransmission Timer, Effectively Dropping the Packet; (cf. [Men+18, pp. 32–34])

- **Difficult** – an attack takes at least a month or that the number of asset samples required to perform the attack is less than one hundred. [Ins11a]
- **None** – the opportunity window is not sufficient to perform the attack. [Ins11a]

ETSI TS 102 165-1 version 4.2.3 [Ins11a] classifies the time factor as follows:

- **≤1 day** – an attack can be identified or exploited in less than one day. [Ins11a]
- **≤1 week** – an attack can succeed in less than a week. [Ins11a]
- **≤1 month** – an attack can succeed in less than a month. [Ins11a]
- **≤3 months** – an attack can succeed in less than three months. [Ins11a]

- **≤6 months** – an attack can succeed in less than six months. [Ins11a]
- **>6 months** – a successful attack requires more than six months. [Ins11a]

ETSI TS 102 165-1 version 4.2.3 [Ins11a] groups the expertise factor as follows:

- **Laymen** are not knowledgeable compared to experts or proficient persons, with no particular expertise. [Ins11a]
- **Proficient** persons are knowledgeable in that they are familiar with the security behavior of the product or system type. [Ins11a]
- **Experts** are familiar with the underlying algorithms, protocols, hardware, structures, security behavior, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type. [Ins11a]

ETSI TS 102 165-1 version 4.2.3 [Ins11a] divides the knowledge factor as follows:

- **Public** information concerning the asset (e.g., as gained from the Internet). [Ins11a]
- **Restricted** information concerning the asset (e.g., knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement). [Ins11a]
- **Sensitive** information about the asset (e.g., knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams). [Ins11a]
- **Critical** information about the asset (e.g., knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need-to-know basis and individual undertaking). [Ins11a]

ETSI TS 102 165-1 version 4.2.3 [Ins11a] categorizes the equipment factor as follows:

- **Standard** equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack. This equipment may be a part of the asset itself (e.g., a debugger in an operating system) or can be readily obtained (e.g., Internet downloads, protocol analyzer, or simple attack scripts). [Ins11a]
- **Specialized** equipment is not readily available to the attacker, but could be acquired without undue effort. This could include the purchase of moderate amounts of equipment (e.g., power analysis tools or the usage of hundreds of PCs linked across the Internet), or development of more extensive attack scripts or programs. [Ins11a]

Attack Intensity	Value
Single instance of attack	1
Moderate level of multiple instances	2
Heavy level of multiple instances	3

Table 6: Attack Intensity Levels [Ins11a]

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

Table 7: Asset Impact Values [Ins11a]

- **Bespoke** equipment is not readily available to the public as it may need to be specially produced (e.g., very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive. [Ins11a]

The level of attack intensity is a factor in determining the impact of an attack [Ins11a]. ETSI TS 102 165-1 version 4.2.3 [Ins11a] classifies the levels of attack intensity as displayed in Table 6.

Modifiers for the attack intensity are the number of attack sources, the time interval between attacks, or a combination of these two. [Ins11a]

The asset impact is a factor in determining the impact of an attack [Ins11a]. The categorization of the asset impact is displayed in Table 7.

7.2.2 Potential of an Attack

To calculate the attack potential, all attack factor values are summed (i.e., Time + Expertise + Knowledge + Opportunity + Equipment) as displayed in Table 8. [Ins11a]

7.2.3 Likelihood of an Attack

The calculated attack potential value maps to the vulnerability rating as shown in Table 9. In turn, this vulnerability rating maps to the likelihood of an attack as of Table 10.

For the later calculation of the risk of an attack, the likelihood of an attack maps to the values displayed in Table 11.

Factor	Range	Value
Time (1 point per week)	≤1 day	0
	≤1 week	1
	≤1 month	4
	≤3 months	13
	≤6 months	26
	>6 months	See note 1
Expertise	Layman	0
	Proficient	2
	Expert	5
Knowledge	Public	0
	Restricted	1
	Sensitive	4
	Critical	10
Opportunity	Unnecessary/unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	See note 2
Equipment	Standard	0
	Specialized	3
	Bespoke	7

Note 1: Attack potential is beyond high. **Note 2**: Attack path is not exploitable.

Table 8: Attack Potential Values [Ins11a]

Attack Potential	Vulnerability Rating
0 to 2	No rating
3 to 6	Basic
7 to 14	Moderate
15 to 26	High
>26	Beyond high

Table 9: Mapping of Attack Potential to Vulnerability Rating [Ins11a]

Vulnerability Rating	Likelihood
No rating	Likely
Basic	
Moderate	Possible
High	Unlikely
Beyond high	

Table 10: Mapping of Vulnerability Rating to Likelihood [Ins11a]

Value	Likelihood	Explanation
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.

Table 11: Likelihood Values [Ins11a]

Asset Impact	Attack Intensity	Attack Impact
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3
3	0	3
3	1	3
3	2	3

Table 12: Attack Impact Calculation [Ins11a]

7.2.4 Impact of an Attack

The impact of an attack results from the addition of the asset impact and the attack intensity. The attack impact is capped at 3. As a result, any sum greater than 3 is given the value 3. All possible combinations of the asset impact and the attack intensity with the resulting attack impact are shown in Table 12.

7.2.5 Establishment of Risk

The risk of an attack is calculated by multiplying the likelihood and the impact of an attack. All possible products of the multiplications of likelihood and impact are mapped to risk as defined in Table 13.

Likelihood * Impact	Risk	Explanation
1, 2	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
3, 4	Major	Threats on relevant assets are likely to occur, although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6, 9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.

Table 13: Risk Calculation [Ins11a]

7.3 Risk of Black Hole Attacks identified in the ETSI Technical Report 102 893

In ETSI TR 102 893 [Ins17b] it is distinguished between risks on a Smart Vehicles and a RSU. Black hole attacks are identified as a threat to availability in Smart Vehicles. Black hole attacks belong to the threat groups *denial of access to outgoing messages* and *modification and deletion of transmitted information*. These threat groups have the following undesired consequences [Ins17b]:

(1) *Accidents if collision warnings are not received and processed by the attacked ITS-S.* [Ins17b]

(2) *General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages.* [Ins17b]

The risk identified for the threat groups *denial of access to outgoing messages* and *modification and deletion of transmitted information* in the TVRA of ETSI TR 102 893 [Ins17b] is displayed in Table 14.

7.4 Security Measures against Black Hole Attacks in ETSI Cooperative Intelligent Transport Systems

The TVRA in ETSI TR 102 893 [Ins17b] describes various security measures. As described in subsection 4.6.2 Technical Specifications of Security Standards and in subsection 4.6.3

Threat Group	Factor	Range	Value	Potential	Likelihood	Impact	Risk
Denial of access to outgoing messages	Time	$\leq$ 1 week	1	8 (Mod.)	2 (Poss.)	3 (High)	6 (Crit.)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Specialized	3				
Modification and deletion of transmitted information	Time	$\leq$ 1 week	1	14 (Mod.)	2 (Poss.)	3 (High)	6 (Crit.)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				

Mod.=Moderate, **Poss.**=Possible, **Crit.**=Critical

Table 14: Risk of Threat Groups of Black Hole Attacks in the ETSI TR 102 893 [Ins17b]

Security Standard Conformance, except for ETSI C-ITS security header-related security measures, no security measures have to be complied with through TS' or are tested through security tests. An implementation of such security measures is optional. The following security measures provide security against black hole attacks [Ins17b]:

(1) *Limit message traffic to V2I/I2V when infrastructure is available and implement message flow control and station registration.* [Ins17b]

(2) *Provide remote deactivation of misbehaving devices capability (includes the capability of detecting misbehaving devices).* [Ins17b]

(3) *Alternative communication path to remove misbehaving devices and to download security management information.* [Ins17b]

(4) *Digitally sign each message using a Kerberos/PKI-like token system.* [Ins17b]

In this thesis security measure (1) is further referred to as *V2I/I2V message restrictions*. The security measures (2) and (3) are intended to be used together. Combined they are referred to as *detection and removal/deactivation of misbehaving ITS stations* in this thesis. In practice, the security measure (4) can be achieved by *enabling the ETSI C-ITS security header*.

7.5 Risk Analysis of Black Hole Attacks on the GeoNetworking Protocol

The risk analysis in this section considers both the risk without security measures and the risk with security measures described in the previous section, namely *V2I/I2V message restrictions*, *detection and removal/deactivation of misbehaving ITS stations*, and *enabling the ETSI C-ITS security header*.

7.5.1 Risk without Security Measures

The risk analysis in this subsection does not consider any security measures that may be present at the current time or are planned to be deployed in the future. The risk of black hole attacks on individual forwarding algorithms is displayed in Table 15. A description of the results shown in Table 15 is given in the following subsections.

Risk on N-Hop Broadcast Forwarding and GeoBroadcast Forwarding

As described in subsection 7.1.1 *N*-Hop Broadcast Forwarding in Topologically Scoped Broadcast and in subsection 7.1.4 GeoBroadcast Forwarding in Simple GeoBroadcast Forwarding, black hole attacks on NHBF and GBF are not possible. As a result, black hole attacks on both forwarding algorithms have an opportunity of *none*. Other factors are not measured, because as black hole attacks cannot be performed, there is no risk of black hole attacks.

Risk on Greedy Forwarding

As described in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding, black hole attacks can be performed on GF.

To send multiple beacons with spoofed information, an attacker would need to adapt an ETSI C-ITS implementation and to have a radio frequency receiver/transmitter to transmit GF packets. As open-source ETSI C-ITS implementations, such as Vanetza [Ingb] by the *Technische Hochschule Ingolstadt*, are readily available, adapting an ETSI C-ITS implementation to send beacons with spoofed information requires little effort. Radio frequency receivers/transmitters are readily available in online shops, such as Amazon starting from ~10 Euros [Inc]. Under the categorization of the equipment factor given in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the equipment required to perform a black hole attack on GF falls into the category *specialized*.

To perform the discovered black hole attack scenario on GF, asset samples in the form of GF packets are required. As GF packets are transmitted over the air, anybody with a radio frequency receiver has unlimited access to GF packets. As a result, anybody with a suitable radio frequency receiver can access them. Following ETSI TS 102 165-1 version 4.2.3 [Ins11a], the opportunity factor of this attack is categorized as *unlimited access*.

The robustness analysis in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding has been performed on entirely public information. Performing this robustness analysis on entirely public information exemplifies that the discovered black hole attack scenario on GF can be performed on entirely public information. Under the categorization of the knowledge factor in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the knowledge factor of the black hole attacks on GF is categorized as *public*.

Any attacker that performs the discovered black hole attack scenario on GF would have to be an expert. To perform the discovered black hole attack scenario on GF, an attacker has

to be familiar with the security behavior of GF, with the GF algorithm, with structures underlying GF (e.g., how location tables are updated or how GeoNetworking addresses and locations can be spoofed), and black hole attacks, which are classical attacks on VANETs (i.e., they are extensively described in current research; e.g., Grimaldo and Martí [GM18], Gokhale et al. [Gok+11], or Chaubey [Cha16]). Given the categorization of the expertise factor in ETSI TS 102 165-1 version 4.2.3 [Ins11a], attackers with such skills are most suitably classified as *experts*.

Without an independent researcher having performed the discovered black hole attack scenario on GF, as described in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding, in practice, it is hard to precisely assess the amount of time required for a successful attack. It is estimated that the attack scenario can be performed in less than a month. Identifying that GF is susceptible to the discovered black hole attack would probably take an expert in the GeoNetworking protocol or anybody who discovers this thesis approximately a day. Obtaining and developing the required equipment likely requires approximately one week. After obtaining and developing the required equipment, the discovered attack scenario could be carried out immediately. Given the categorization of the time factor in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the time factor of a black hole attack on GF is categorized as *≤1 month*.

The sum of the values of all factors leads to an attack potential of 12 (*moderate*). This attack potential value maps to the likelihood *possible*.

Because black hole attacks on GF can lead to fatal traffic accidents [Qu+15], they result in severe damage and are a threat to the basis of the business of the underlying asset (i.e., ETSI C-ITS). Given the calculation of the attack impact in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the attack impact of black hole attacks on GF is *high* regardless of the attack intensity.

Calculating the risk of a black hole attack on GF from the attack's likelihood (*possible:* 2) and the attack's impact (*high:* 3) results in a value of 6 (*critical*).

Risk on Contention-Based Forwarding

As described in subsection 7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast, black hole attacks could, in theory, be performed on CBF. For the purpose of this risk analysis, it is assumed that the discovered black hole attack scenario on CBF is feasible in practice.

To perform the discovered black hole attack scenario on CBF, physical simulation of packet transmission, one or multiple highly precise directional antennas, a radio frequency receiver, and an attack script/program are required. Open-source physical simulation software, such as Veins by Sommer et al. [Som+] and INET by Bojthe et al. [Boj+a], make physical simulations easily accessible to the public. An attacker can use such, or similar readily-available software, to identify ITS stations with an active retransmission timer. The number and the required precision of the necessary directional antennas heavily

influence the costs of performing the discovered black hole attack scenario. Directional antennas and radio frequency receivers are readily available in online shops, such as Amazon for prices starting from ~7 Euros [Inc]. Directional antennas near the starting price should be expected to have relatively low precision, while higher-priced antennas likely have higher precision. Without simulations or field tests of the discovered attack scenario, the required amount and the required precision of directional antennas cannot be specified precisely. In a best-effort attempt, it is estimated that a moderate amount (i.e., 6 to 10) of directional antennas with moderate precision would be required to perform the attack scenario. It is further estimated that the required attack script/program would be moderately difficult to develop. Such an attack script/program requires to (1) automatically use simulation software, (2) interpret the results of this simulation, and (3) appropriately control the employed directional antennas. Developing such a script/program is arguably neither very easy nor very difficult. Under the categorization of the equipment factor given in ETSI TS 102 165-1 version 4.2.3 [Ins11a], equipment that consists of easily accessible simulation software, moderate amounts of directional antennas, and an attack script/program that is moderately difficult to develop would most fittingly be categorized as *specialized*.

To perform the discovered black hole attack scenario, asset samples in the form of CBF packets are required. Analogously to GF packets, CBF packets are transmitted over the air. Under the categorization of the opportunity factor given in ETSI TS 102 165-1 version 4.2.3 [Ins11a] such unlimited access falls into the category *unnecessary/unlimited access*.

The robustness analysis in subsection 7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast has been conducted on entirely public information. Conducting this robustness analysis on public information shows that an attacker can perform a black hole attack on CBF on entirely public information. Following the categorization of the knowledge factor given in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the knowledge factor of the discovered black hole attack scenario on CBF is categorized as *public*.

The robustness analysis in subsection 7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast shows that an attacker has to be familiar with the CBF algorithm, specialized equipment, such as directional antennas, the security behavior of CBF, and black hole attacks. Under the categorization of the expertise factor specified in ETSI TS 102 165-1 version 4.2.3 [Ins11a] attackers with such skills are classified as *experts*.

Without an independent researcher having performed the discovered black hole attack scenario on CBF in practice, the amount of time required for a successful attack cannot be precisely assessed. It is estimated that the discovered black hole attack scenario could be performed in less than a month, given the attacker already has the required knowledge to perform the attack scenario. Identifying that CBF is susceptible to the discovered black hole attack scenario would likely take about a day, given an attacker is an expert on the GeoNetworking protocol or reads this thesis. Obtaining and developing the required equipment would probably require around two weeks. After obtaining and developing the required equipment, the discovered black hole attack scenario could be carried out

Threat	Factor	Range	Value	Potential	Likelihood	Impact	Risk
Black Hole Attack on NHBF	Time	N/A	N/A	N/A	N/A	N/A	None
	Expertise	N/A	N/A				
	Knowledge	N/A	N/A				
	Opportunity	None	N/E				
	Equipment	N/A	N/A				
Black Hole Attack on GF	Time	$\leq$ 1 month	4	12 (Mod.)	2 (Poss.)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Public	0				
	Opportunity	Unlimited Access	0				
	Equipment	Specialized	3				
Black Hole Attack on CBF	Time	$\leq$ 1 month	4	12 (Mod.)	2 (Poss.)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Public	0				
	Opportunity	Unlimited Access	0				
	Equipment	Specialized	3				
Black Hole Attack on GBF	Time	N/A	N/A	N/A	N/A	N/A	None
	Expertise	N/A	N/A				
	Knowledge	N/A	N/A				
	Opportunity	None	N/E				
	Equipment	N/A	N/A				

Mod.=Moderate, **Poss.**=Possible, **N/A**=Not Applicable, **N/E**=Not Exploitable

Table 15: Risk of Black Hole Attacks without Security Measures

immediately. Given the categorization of the time factor in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the time factor of a black hole attack on CBF is categorized as *$\leq$1 month*.

Summing the values of each factor leads to a vulnerability rating, also known as attack potential, of 12 (*moderate*). This attack potential value maps to the likelihood *possible*.

Analogously to the argumentation of the attack impact in the subsubsection Risk on Greedy Forwarding of this section, the attack impact of black hole attacks on CBF is *high*.

Multiplying the likelihood of a black hole attack on CBF (*possible:* 2) and the impact of such an attack (*high:* 3) results in a value of 6 (*critical*).

7.5.2 Risk with Vehicle-To-Infrastructure/Infrastructure-To-Vehicle Message Restrictions

In urban and highway areas, ETSI C-ITS infrastructure is expected to be deployed relatively soon [Env16]. With ETSI C-ITS infrastructure in place and enforced V2I/I2V message restrictions, malicious ITS stations would not be able to absorb traffic as

required for phase (1) of black hole attacks. In areas with ETSI C-ITS infrastructure, black hole attacks could be fully prevented by V2I/I2V message restrictions [Ins17b]. However, infrastructure is not expected to be widely available in rural areas in the near future [Env16].

As a result, to adequately address black hole attacks in GF and CBF as a whole V2I/I2V message restrictions alone are not sufficient. In areas with ETSI C-ITS infrastructure and enforced V2I/I2V message restriction, the opportunity of black hole attacks would be *none* for GF and CBF under the opportunity factor categorization given in ETSI TS 102 165-1 version 4.2.3 [Ins11a]. An opportunity factor of *none* means there would be no risk of black hole attacks. In areas without infrastructure, risk would be present as in Table 15.

7.5.3 Risk with Detection and Removal/Deactivation of Misbehaving ITS stations

With *detection and removal/deactivation of misbehaving ITS stations*, ITS stations that cause problems to other ITS stations can be deactivated and/or removed from the routing process. It will not be possible to deactivate specialized hardware designed to attack ETSI C-ITS. Specialized hardware designed to attack ETSI C-ITS will have to be removed from the routing process to mitigate/prevent an attack. [Ins17b]

Due to technical limitations in misbehavior detection, the detection of misbehaving ITS stations may not be timely or definitive [Ins17b]. These technical limitations include time delays in trust-based misbehavior detection and problems in attack discovery (i.e., false positive or false negative classification of events or ITS stations), as discussed by van der Heijden et al. [Hei+18a]. As a result, the discovered black hole attack scenarios on GF and CBF can still be performed for a limited time and/or when an attack/attacker is misclassified as not being an attack/attacker. Due to the potential indefiniteness of misbehavior detection, these solutions introduce a new risk: Vehicles may be falsely classified as misbehaving. Misbehavior detection is discussed in more detail in section 9.6 Misbehavior Detection in Vehicular Ad Hoc Networks.

As there is no factor for time limitation or misclassification in ETSI TS 102 165-1 version 4.2.3 [Ins11a], the risk of a black hole attack on GF or CBF with the security measure of *detecting and removing/deactivating misbehaving ITS stations* cannot be described with the employed methodology.

7.5.4 Risk with an Enabled ETSI Cooperative Intelligent Transport Systems Security Header

The usage of the ETSI C-ITS security header as defined in ETSI TS 103 097 [Ins17d] affects black hole attacks on GF differently than black hole attacks on CBF. In the context of black hole attacks, the only relevant feature of the ETSI C-ITS security header is a signature on every GeoNetworking packet. The encryption of GeoNetworking packets

would not influence black hole attacks. Signatures on GeoNetworking packets provide integrity to each packet and guarantee that the sender of a packet is authentic [Ins17d]. The signature in an ETSI C-ITS security header is linked to the GeoNetworking address of an ITS station [Ins10c].

Risk on Greedy Forwarding

In the discovered black hole attack scenario on GF, the ETSI C-ITS security header would prevent black hole attacks. As discussed in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding, the discovered black hole attack scenario on GF relies on a lack of authenticity of the location table that allows an attacker to spoof numerous ITS stations. This spoofing process involves faking the GeoNetworking address for the spoofed ITS stations. As signatures are linked to the GeoNetworking address of an ITS station [Ins10c], an attacker could no longer fake the GeoNetworking address for spoofed ITS station without invalidating the signature. As a result, an attacker that only possesses certificates that are intended for their ITS station could no longer spoof ITS stations, but only spoof one location. As described in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding the capability of spoofing their own location only allows to perform phase (1) and phase (2) of a black hole attack for a packet sent in a specific direction. Only performing phase (1) and phase (2) of a black hole attack for a packet sent in a specific direction does not constitute a black hole attack. As a result, the discovered black hole attack scenario on GF is not possible when the ETSI C-ITS security header is enabled. As the discovered black hole attack scenario is not possible on GF, black hole attacks on GF have an opportunity of *none* under the categorization of the opportunity factor given in ETSI TS 102 165-1 version 4.2.3 [Ins11a].

Risk on Contention-Based Forwarding

In the discovered black hole attack scenario on CBF, the ETSI C-ITS security header would provide no additional security. The discovered black hole attack scenario on CBF is not based on violating the integrity of a packet or sending unauthentic messages. Instead, as described in subsection 7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast, the discovered black hole attack scenario is based on the inability of intermediary recipients to easily check if an ITS station only retransmitted a packet in a targeted manner or actually rebroadcasted the packet. As a result, the ETSI C-ITS security header does not affect the security of the discovered black hole attack scenario on CBF. The risk of black hole attacks on CBF with an enabled ETSI C-ITS security header is the same as without any security measures, as displayed in Table 15.

CHAPTER 8

Simulation of Black Hole Attacks in ETSI Cooperative Intelligent Transport Systems

This chapter covers (1) a discussion of selection criteria and the selection process of an ideal ETSI C-ITS implementation and a suitable VANET simulator, (2) the setup process of the selected ETSI C-ITS implementation and the VANET simulator, as well as the integration of the ETSI C-ITS implementation into the VANET simulator, (3) the development of black hole attack functionality in the selected ETSI C-ITS implementation, and (4) a definition of selection criteria for an ideal data set for this thesis, the selection process of an ideal data set, and the integration of the selected data set into the selected ETSI C-ITS implementation and the selection VANET simulator. The combination of an ETSI C-ITS implementation and a VANET simulator is further referred to as ETSI C-ITS simulation framework.

Task (1) is done separately for ETSI C-ITS implementations and VANET simulators. The main functionality of an ETSI C-ITS simulation framework lies in the ETSI C-ITS implementation. As such, a special focus lies on the selection process of an ETSI C-ITS implementation. Not only the selection criteria and the selection process of an ETSI C-ITS implementation are discussed, but also the software components of the selected ETSI C-ITS implementation. For the selection process of VANET simulators, several selection criteria are defined and evaluated.

Task (2) is performed on a Linux virtual machine, more specifically on Ubuntu 18.04.

Because black hole attacks do not belong to the functionality of the ETSI C-ITS standard set, it is expected that task (3) is not already possible in the selected ETSI C-ITS implementation and needs to be developed separately.

8.1 Selection Criteria of ETSI Cooperative Intelligent Transport Systems Implementations

Some vendors keep ETSI C-ITS implementations closed-source (e.g., ezCar2x by Roscher et al. [Ros+13] or VSimRTI by Nauman et al. [Nau+09]). However, there are also open-source ETSI C-ITS implementations (e.g., OpenC2X by Laux et al. [Lau+16], GeoNet Stack by Voronov et al. [Vor+b; Vor+a], or Vanetza [Ingb]). In contrast to open-source implementations, closed-source implementations cannot be assessed for their suitability for black hole attacks easily beforehand and complicate the reproduction of results in follow-up research. For these reasons, only open-source implementations are considered in this thesis.

The selection of an ideal ETSI C-ITS implementation for black hole attacks requires to consider various criteria that are defined in the following of this section. The criteria are ordered by importance.

8.1.1 ETSI Cooperative Intelligent Transport Systems Functionality Support

As black hole attacks in VANETs are performed on the network layer, a suitable ETSI C-ITS implementation needs to (1) support GeoNetworking. For developers of ETSI C-ITS applications to be able to test their implementation in a simulation, (2) V2X messaging (i.e., CAM and DENM) on the facilities layer. As the DCC [Aut+13] and the ETSI C-ITS security header [LC16] influence the overall performance and the security behavior of ETSI C-ITS, (3) DCC and ETSI C-ITS security header functionality is required. The support of functionality (1) is crucial. Without functionality (1) simulations of black hole attacks would be impossible. The support of functionality (2) is important. Without functionality (2) developers could not test their application, which would conflict with the motivation of this thesis to provide developers with publicly available means to test their applications. The support of functionality (3) is important. A lack of support of functionality (3) would diminish the realism of black hole attack simulations which would conflict with the motivation of this thesis to provide black hole attack simulations with relatively high realism.

8.1.2 Integration into a Vehicular Ad Hoc Network Simulator

Tests of black hole attacks could either be done with field testing and experimentation in the real world or in a VANET simulator [Lau+16]. Since real-world security tests of VANETs are costly [Rie+15], a potentially suitable ETSI C-ITS implementation needs to be easily integrable into a VANET simulator. Optimally, a setup process would already be documented in current research or on the Internet. Without an easy integration into a VANET simulator, developers and security researchers who want to test for security against black hole attacks would have to overcome non-negligible integration overhead. Fulfilling this criterion is important. Even if the criterion is not fulfilled, black hole attack

simulations could be performed. However, the integration overhead for developers and security researchers would conflict with the motivation of this thesis to allow developers and security researcher to easily test for security against black hole attacks.

8.1.3 Continued Maintenance and Good Extensibility

The release 1 of ETSI C-ITS has been standardized in 2010. There have been a few early ETSI C-ITS implementations (e.g., VSimRTI [Nau+09] or iTetris [Goz+09], both in 2009). Some of these are outdated and/or not maintained anymore (e.g., iTetris, as visible on its website [PC]). A suitable ETSI C-ITS implementation should be easily extensible but also still be maintained to this date by a major contributor to the code base. The criteria *continued maintenance* and *good extensibility* are desirable. Without continued maintenance and good extensibility the extension of the work in this thesis would be impeded. Such an impediment would not conflict with any motivation of this thesis, but it should be considered bad practice to produce research that cannot be easily reproduced and extended.

8.2 Selection Process of ETSI Cooperative Intelligent Transport Systems Implementations

OpenC2X, GeoNet Stack, and Vanetza [Ingb] are well-known open-source implementations of ETSI C-ITS in current research (e.g., Riebl et al. [Rie+17] or Laux et al. [Lau+16]). They are considered in the following selection process.

8.2.1 Evaluation of the ETSI Cooperative Intelligent Transport Systems Functionality Support

The fulfillment of functionality requirements of OpenC2X [Lau+16], GeoNetStack [Vor+b; Vor+a], and Vanetza [Rie+17] is displayed in Table 16. OpenC2X does not support the GeoNetworking protocol and the ETSI C-ITS security header [Lau+16]. GeoNet Stack does not support DCC and the ETSI C-ITS security header [Vor+b; Vor+a]. Both, OpenC2X and GeoNet Stack, do not fulfill the selection criterion *ETSI C-ITS functionality support*. As a result, the selection criteria *integration into a VANET simulator* and *continued maintenance and good extensibility* are not evaluated for OpenC2X and GeoNet Stack. Vanetza supports all required ETSI C-ITS functionality.

8.2.2 Evaluation of the Integration into a Vehicular Ad Hoc Network Simulator, Continued Maintenance, and Good Extensibility

Vanetza does not depend on any specific VANET simulator [Rie+17]. However, Vanetza has been designed to easily integrate into the well-known simulator Objective Modular Network testbed in C++ (OMNet++) [Rie+19]. Vanetza is still maintained by a major contributor to this date, as visible on the GitHub page of Vanetza [Ingb]. Conceptually, Vanetza is an open implementation, designed for extensibility [Rie+17].

ETSI	Standard	OpenC2X	GeoNet Stack	Vanetza
GeoNetworking	102 636-4-2	✗	✓	✓
CAM	102 637-2	✓	✓	✓
DENM	102 637-3	✓	✓	✓
DCC	102 687	✓	✗	✓
ETSI C-ITS Security Header	103 097	✗	✗	✓

✓ Supported, ✗ Not Supported

Table 16: Functionality of well-known open-source ETSI C-ITS Implementations

Requirement	OpenC2X	GeoNet Stack	Vanetza
ETSI C-ITS Functionality Support	✗	✗	✓
Integration into VANET Simulators	–	–	✓
Continued Maintenance	–	–	✓
Extensibility	–	–	✓

✓ Fulfilled, ✗ Not Fullfilled, – Not Evaluated Further

Table 17: Fulfillment of Selection Criteria of each Evaluated ETSI Cooperative Intelligent Transport Systems Implementation

8.2.3 Selected ETSI Cooperative Intelligent Transport Systems Implementation

Vanetza is the only suitable ETSI C-ITS implementation for this thesis. It implements all required functionality, is easily integrable into a VANET simulator, is still maintained to this date, and is designed to be extended. The other implementations, OpenC2X and GeoNet Stack, do not fulfill the selection criterion *ETSI C-ITS functionality support* and as a result, cannot be considered for the work in this thesis. Table 17 provides an overview of the fulfillment of selection criteria for each evaluated ETSI C-ITS implementation.

8.3 Stack of the Selected ETSI Cooperative Intelligent Transport Systems Implementation

Vanetza belongs to an implementation stack including Artery and Veins/INET, as displayed in Figure 25. On the lowest layers, Veins and INET enable the simulation of physical and MAC layer functionality. Veins models the U.S. American standard and mostly exists Vanetza's implementation stack historically. Higher on the stack, Vanetza controls the DCC and implements the ETSI C-ITS network and transport layer together with a horizontal security layer. On top of that, the Artery framework provides facilities and application layer functionality. [Rie+19]

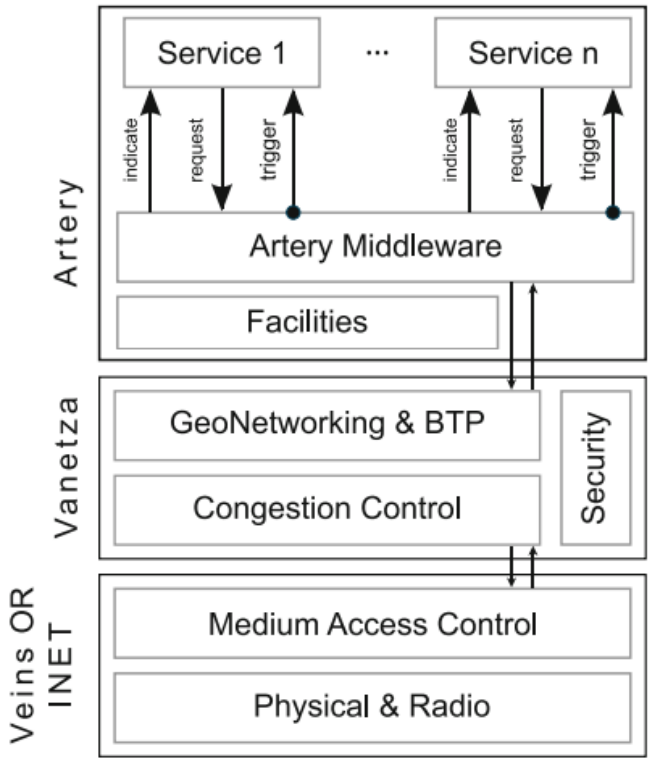


Figure 25: Stack of the Selected ETSI Cooperative Intelligent Transport Systems Implementation [Rie+19]

As an open implementation, Vanetza is optimal for the implementation of experimental features. Such features may be variations of existing, standardized, or entirely new features. [Rie+17]

8.4 Selection Criteria of Vehicular Ad Hoc Network Simulators

Simulating black hole attacks with Vanetza requires a fitting VANET simulator. For the same reasons as stated in section 8.1 Selection Criteria of ETSI Cooperative Intelligent Transport Systems Implementations Implementations, only open-source VANET simulators are considered.

An ideal open-source VANET simulator shall fulfill the following criteria. The criteria are ordered by importance.

8.4.1 Support of Traffic Simulations

An ideal VANET simulator not only allows network simulation, but also traffic simulation. It is desirable that the selected VANET simulator either includes a traffic simulator or easily integrates a traffic simulator. Without traffic simulation, black hole attack simulations cannot be performed. As a result, this criterion is crucial.

8.4.2 Easy Integration of Vanetza

As Vanetza will be used for simulations, an optimal VANET simulator must easily integrate Vanetza and its related stack. Although the fulfillment of this criterion is not crucial, it is important. A lack of easy integration would cause significant integration overhead for developers and security researchers. This would conflict with the motivation of this thesis to allow developers and security researchers to easily test for security against black hole attacks.

8.5 Selection Process of Vehicular Ad Hoc Network Simulators

In current research there are three major open-source simulators: OMNet++ (e.g., Varga [Var10], Obermaier and Facchi [OF17], or Riebl et al. [Rie+19]), Network Simulator 3 (NS-3; e.g., Riley and Henderson [RH10], Bittl [Bit17], or Riebl et al. [Rie+19]), and VANETSim (e.g., Tomandl et al. [Tom+14] or Bittl [Bit17]).

OMNet++ does not support traffic simulations on its own. The traffic simulator Simulation of Urban MObility (SUMO) easily integrates into OMNet++ [Som+08]. NS-3 also does not support traffic simulations directly but can be easily complemented by SUMO [AW10]. VanetSim comes with its own traffic simulator [Tom+14].

There is no specific obstacle for the integration of Vanetza into NS-3 or VANETSim. However, Vanetza has been specifically designed to be used with OMNet++. [Rie+17]

OMNet++, NS-3, and VanetSim are all suitable for the work in this thesis. They all easily integrate a traffic simulator or include a traffic simulator. However, OMNet++ has a slight advantage over NS-3 and VanetSim, as Vanetza is specifically designed to be used with OMNet++. For that reason, this thesis further uses OMNet++.

8.6 Setup of the Selected Vehicular Ad Hoc Network Simulator and the Selected ETSI Cooperative Intelligent Transport Systems Implementation

The setup of the selected ETSI C-ITS simulation framework in this section is performed on a virtual machine with a 64-bit Ubuntu 18.04 operating system.

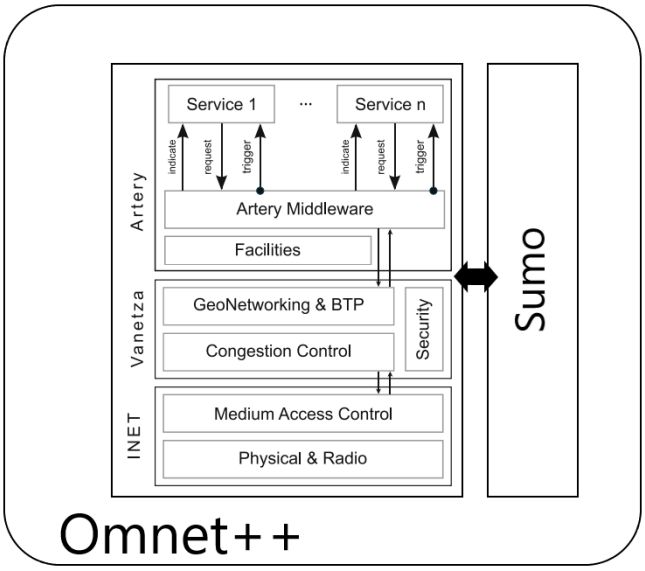


Figure 26: Full Stack of the Selected Simulation Framework (c.f. [Rie+19])

Figure 26 displays the full stack of the selected simulation framework. The ETSI C-ITS implementation stack and the traffic simulator SUMO reside in the simulator OMNet++. As SUMO simulates traffic on the ETSI C-ITS implementation stack, there is an interaction between SUMO and the ETSI C-ITS implementation stack.

8.7 Development of Black Hole Attack Functionality

As discussed in chapter 7 Security of the GeoNetworking Protocol against Black Hole Attacks, black hole attacks can be performed on GF and CBF. While GF is used in GeoUnicast, GeoAnycast, and the GeoUnicast phase of Simple GeoBroadcast Forwarding, CBF is used in GeoUnicast and GeoAnycast.

The selected stack (and any other potentially suitable implementation stack) currently does not support standalone GeoUnicast or GeoAnycast to an extent that could be implemented in the scope of this thesis. As a result, black hole attack functionality can currently not be specifically developed for GeoUnicast and GeoAnycast. By elimination, black hole attack functionality can only be specifically developed for GF that is used in the GeoUnicast phase of Simple GeoBroadcast Forwarding. The functionality is developed in a way that is believed to allow black hole attacks in GeoUnicast and GeoAnycast as soon as they are fully implemented. At that time, as GF is a direct competitor to CBF, it will be interesting to compare the network performance GF and CBF under black hole attacks. In foresight of this comparison, the black hole attack functionality developed in this thesis shall allow enforcing either GF or CBF globally as a GeoUnicast forwarding algorithm.

Software	Commit Hash
Vanetza	cf36ccc72cc3333aa35935e9074acfa3502adae1
Artery	cab1dac3cb75c7599f1c960bd23f96061f0943a4
INET	1032e2666f081e1f0e8ff742969403fce2353d0c
Veins	550e2462ade4e665805abcc829bde131878c3d0b
Pybind11	9a19306fbf30642ca331d0ec88e7da54a96860f9
SimuLTE	e49d7ff2f92c1f80f201c8a53ff13adef57091e9

Table 18: Commit Hashes of the Used Software

The black hole attack functionality developed in this thesis is important preliminary work for achieving the goal of enabling black hole attacks in ETSI C-ITS. The developed functionality can be used by anybody to develop a black hole attack scenario. For example, a researcher who wants to perform a black hole attack in ETSI C-ITS can use the developed functionality to develop a black hole attack scenario for GF, such as the ones described in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding or in subsection 7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast.

The source code of Vanetza [Ingb] and Artery [Inga] used for the modification in this thesis is obtained from their GitHub repositories respectively. Artery is used with INET version 3.6.5 from a forked GitHub repository [Boj+b], with Pybind11 version 2.2.4 from its GitHub repository [Jak+], with SimuLTE from a forked GitHub repository [Vir+], and with Veins from its GitHub repository [Som+]. The hashes of the used commits are displayed in Table 18.

The black hole attack functionality developed in this thesis can be divided as follows:

- Dropping GF/CBF packets
- Enforcing either GF or CBF globally

Dropping GF/CBF packets can be done by introducing a Boolean variable in the per-vehicle Management Information Base (MIB) in *extern/vanetza/geonet/mib.cpp* and *extern/vanetza/geonet/mib.hpp*. The Vanetza router of each ITS station, located in *extern/vanetza/geonet/router.cpp*, must refrain from forwarding GeoUnicast packets depending on the Boolean variable, i.e., discard GeoUnicast packets instead of forwarding them. The Vanetza router is responsible for handling incoming and outgoing packets for an ITS station. [Ingb]

Even though applications can individually specify the used GeoUnicast forwarding algorithms in ETSI C-ITS [Inga], it is advantageous for simulations to be able to globally enforce them. For that, the desired GeoUnicast forwarding algorithm must be set in the MIB [Inga]. This can be achieved by modifying Artery's router in

src/artery/networking/Router.cc to set the itsGnNonAreaForwardingAlgorithm from a configuration parameter [Inga]. Artery's router is responsible for handling messages on the facilities layer [Inga].

8.8 Data Set with a Realistic Traffic Scenario for Black Hole Attacks

In the following of this section, selection criteria for data sets for black hole attacks are defined. In the subsequent selection process, an ideal data set is selected for the integration into the previously selected ETSI C-ITS simulation framework.

8.8.1 Selection Criteria of Data Sets

There are the following selection criteria for data sets in this thesis. These criteria are ordered by importance.

Realistic and Complex Traffic Scenario

Many current performance analyses of black hole attacks in VANETs (e.g., Afdhal et al. [Afd+17], Grimaldo and Martí [GM18], Tyagi and Dembla [TD17], Hamid and Mokhtar [HM15], or Purohit et al. [Pur+17]) rely on small-scale subscenarios of complex traffic scenarios as they occur in the real world (e.g., in the city of Luxembourg [Cod+17] or in the principality of Monaco [CH18]). Complex traffic scenarios as they occur in the real world are a mix of a variety of small-scale subscenarios [Cod+17]. Due to many performance analyses' reliance on small-scale subscenarios, their results cannot be generalized unequivocally and must be viewed with care [Cod+17]. When simulating small-scale subscenarios, performance can only be measured for the selected subscenarios [Cod+17]. The results of such performance analyses are not necessarily fully representative of more complex traffic scenarios [Cod+17].

A suitable data set for this thesis should use a realistic traffic scenario, as described in section 6.2 Black Hole Attacks in Vehicular Ad Hoc Networks, but instead of having *at least one small-scale subscenario of either an urban area, a highway, or a rural area*, the traffic scenario is expected to be a mix of a variety of small-scale subscenarios (i.e., to be a complex traffic scenario) of either an urban area, a highway, or a rural area. The usage of a complex traffic scenario allows to generalize results for the used area (i.e., urban area, highway, or rural area) [Cod+17].

Using a realistic traffic scenario is important. Though black hole attack simulations could be conducted without a realistic traffic scenario, the lack of a realistic traffic scenario would conflict with the motivation of this thesis to provide developers of ETSI C-ITS applications and ETSI C-ITS security researchers with a realistic traffic scenario. Using a complex traffic scenario is important because it allows developers and security researchers to generalize their results. As a result, developers and security researchers do not have

to test for security against black hole attacks in a variety of small-scale subscenarios at once, which arguably requires significantly lower effort (i.e., easier) than testing in multiple independent small-scale subscenarios.

Easy Integration into the Selected Simulation Framework

The selected data set must be easily integrable into the selected simulation framework. This criterion is important. A lack of easy integration would conflict with the motivation of this thesis to allow developers and security researchers to easily test for security against black hole attacks.

8.8.2 Selection Process of Data Sets

The SUMO website [Cen] list the following data sets with complex traffic scenarios: the Bologna data set, the Luxembourg SUMO Traffic (LuST) data set, the Monaco SUMO Traffic (MoST) data set, the Travel and Activity PAtterns Simulation (TAPAS) Cologne data set, and the Bologna Ringway data set, which is a continuation of the work in the Bologna data set.

The Bologna data set and the Bologna Ringway data set are relatively small [Cen]. The Bologna Ringway data set is known to have some invalid junction definitions. The invalidity of some junction definitions decreases the realism of the simulation [Cen]. As the Bologna Ringway data set is based on the Bologna data set, it is not unlikely that the Bologna data set suffers from this problem as well [Cen]. As a result, neither the Bologna data set nor the Bologna Ringway data set are well-suited for the work in this thesis.

The TAPAS Cologne data set consists of a complex traffic scenario [CH18]. The TAPAS Cologne data set has a somewhat flawed network [CH18]. For example, the TAPAS Cologne data set has road information that is not consistent with reality and has unrealistic traffic demand [MS15, pp. 325-326]. More specifically, the traffic in the used traffic scenario is unrealistically bursty [MS15, pp. 325-326]. The flawed network leads to a diminished realism of the TAPAS Cologne data set. As a result, the TAPAS Cologne data set is not well-suited for the work in this thesis.

Though the MoST data set is of high quality, it cannot be used in this thesis. The MoST data set does not easily integrate into the selected simulation framework. Out-of-the-box, an integration leads to failing timing assertions of SUMO and/or OMNet++.

The LuST data set has been fine-tuned and hand-checked to provide realistic and reliable data. Its mobility has been verified with real-world data. The LuST data set is widely used in VANET simulations (e.g., Khodaei and Papadimitratos [KP16], Kubička et al. [Kub+16], or van der Heijden et al. [Hei+18b]), though it does not provide elevation information and traffic simulation focuses only on vehicles, neglecting pedestrians. [CH18]

Despite minor limitations, the LuST data set is the most suitable scenario for the work in this thesis. The road pattern of the LuST data set is depicted in Figure 27.

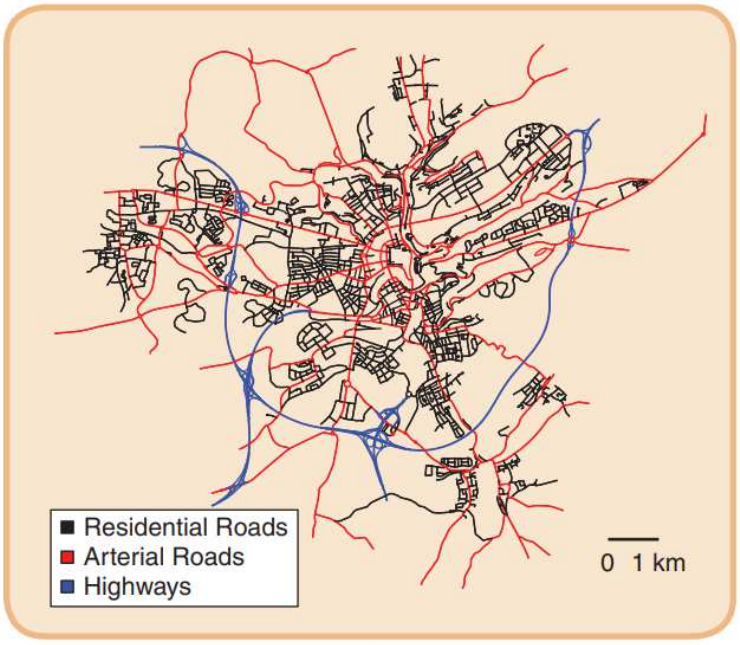


Figure 27: Road Pattern of the LuST Data Set [Cod+17]

8.9 Setup of the Selected Data Set

The setup of the selected data set can be divided as:

- Adding the LuST Data Set to the Scenarios of Artery
- Adding a Base Load to the Network
- Setting an Attacker/Smart Vehicle Ratio

The LuST data set can be obtained from its GitHub repository [Cod+]. In this thesis, the LuST data set is used in the commit *3c90b337005e4bb5edbc5c26da87ecbf94a71687* of release 2.0. To integrate the LuST data set into the simulation framework, it must be added to the scenarios of Artery and build instruction for the LuST data set must be specified. Afterward, Artery has to be rebuilt.

As argued in subsection 6.2.1 Robustness of Well-Known Vehicular Ad Hoc Network Routing Protocols, using a realistic traffic scenario inherently leads to VANET simulations with relatively high realism. To further increase this realism, base loads should be added to the VANET. In Vanetza's stack, Artery's predefined CAM service *artery.application.CaService* and Artery's predefined DENM service can be used to create such a base load. Artery's predefined CAM service *artery.application.CaService* and Artery's predefined DENM service *artery.application.DenService* can be enabled through OMNet++ configuration.

With the CAM service enabled, all ITS stations will periodically send beacons. The DENM service would provide day-1 DENM use cases, such as an impact reduction use case or a traffic jam use case. However, in the current version of Artery enabling the DENM service incorrectly leads to behavior that is inconsistent with the ETSI C-ITS standard. In the predefined use cases, messages are disseminated via Simple GeoBroadcast Forwarding in a circular area around the initially sending ITS station. As a result, there should be no GeoUnicast phase, but only a GeoBroadcast phase. During simulations, however, GeoUnicast forwarding related to the DENM service was observed.

The attacker/node ratio, the node speed, and the attacker proximity significantly influence the results of a black hole attack, as discussed in subsection 6.1.1 Security-Relevant Properties. These properties have to be fixed for reproducibility. Artery allows setting a vehicle ratio based on vehicle types. As a result, to set an attacker/Smart Vehicle ratio, it is only required to have a clear definition of non-malicious and malicious Smart Vehicles. Out-of-the-box Artery has already defined non-malicious Smart Vehicles in *artery.inet.Car*. Malicious Smart Vehicles can be defined by extending *artery.inet.Car* appropriately. The attacker/Smart Vehicle ratio can be set in the OMNET++ configuration of a scenario. The distribution of this ratio must be set with Random Number Generators (RNGs) to ensure that in consecutive runs of the same scenario the same Smart Vehicles are non-malicious/malicious Smart Vehicles. These measures also fix node speed and attacker proximity.

CHAPTER 9

Related Work

This chapter gives an overview of state-of-the-art research related to this thesis.

9.1 Dedicated Short-Range Communication with Wireless Access in Vehicular Environments

Parallel to the European ETSI C-ITS standard set, the U.S. developed its own standard set for VANETs: DSRC with WAVE [Fes15]. J. Kenney [Ken11] provides an extensive description of DSRC with WAVE. The author describes the entire stack from the physical layer to the application layer. Conceptually, the DSRC with WAVE stack is very similar to the ETSI C-ITS stack [Fes15]. However, exact specifications frequently differ slightly [Fes15]. For example, on the physical layer, the reserved radio frequencies of channels differ slightly between DSRC with WAVE and ETSI C-ITS [Fes15]. Higher on the stack on the network and the transport layer, the Wave Short Message Protocol standards are the counterpart to GeoNetworking and BTP in ETSI C-ITS [Fes15]. Similar to ETSI C-ITS, DSRC with WAVE defines a security standard [Fes15]. This security standard is specified by the Institute of Electrical and Electronics Engineers (IEEE) and is referred to as 1609.2 [Fes15].

In 2006, Laurendeau and Barbeau [LB06] analyzed the security of DSRC with WAVE according to the threat analysis method of ETSI TS 102 165-1 version 4.1.1 [Ins03]. They identified (1) malware, (2) black hole attacks, (3) GPS spoofing, and (4) location tracking as critical threats. (5) DoS attacks are considered a major threat. The same threats are considered in the TVRA of ETSI TR 102 893 [Ins17b]. Laurendeau and Barbeau suggest employing trusted computing mechanisms to cope with threat (1). Threat (2) may be prevented by a concept called passive acknowledgment. In this concept, the sending ITS station listens to its neighbors' retransmission to ensure that they have repeated the message. Other measures to prevent threat (2) include multi-path routing or using backup routes. Threat (3) could be prevented by using specialized receivers that access

an authenticated GPS signal. Threat (4) remained an open issue. To mitigate threat (5), the authors recommend requiring ITS stations to perform proof-of-works similar to those by Dwork and Naor [DN92] and employ directional antennas that minimize the number of broadcast messages. Proof-of-works would require a DoS attacker to perform computationally expensive tasks before they could cause computationally expensive tasks on a victim device. In comparison, the TVRA of ETSI TR 102 893 similarly suggests employing trusted computing mechanisms to cope with threat (1). To cope with threat (2), the TVRA suggests the measures described in section 7.4 Security Measures against Black Hole Attacks in ETSI Cooperative Intelligent Transport Systems. For the prevention of threat (3), the TVRA discusses the introduction of GNSS correction systems that would remove the possibility of GPS spoofing. The suggestions of the TVRA to prevent threat (4) are described in subsection 4.6.2 Technical Specifications of Security Standards. To mitigate threat (5), the TVRA [Ins17b] suggests:

- to *limit message traffic to V2I/I2V when infrastructure is available and implement message flow control and station registration,*
- to *include a sequence number in each new message,*
- to *reduce the frequency of beacon and other repeated messages when flow control is not available,*
- to *add source identification across the stack in ITS messages,*
- to *provide remote deactivation of misbehaving devices capability (includes capability of detecting misbehaving devices),*
- to *provide an alternative communication path to remove misbehaving devices and to download security management information, and*
- to *implement frequency agility within the G5A frequency band.* [Ins17b]

More recently, in 2018, Chen et al. [Che+18] perform a security analysis of the so-called Intelligent Traffic Signal System (I-SIG) in DSRC with WAVE in its default configuration. The I-SIG performs traffic signal control based on Smart Vehicle trajectory. As such the I-SIG is similar to the TLC service of ETSI C-ITS, which enables prioritization of public transport and public safety vehicles on signalized road infrastructure, as described in subsection 4.4.2 Vehicle-To-Infrastructure/Infrastructure-To-Vehicle Messaging. In a study under the lead of the University of Arizona [Mmi], the I-SIG has been shown to reduce the delay at intersections by 26.6%. Chen et al. [Che+18] try to perform a congestion attack, i.e., an attack where an attacker maliciously creates congestion. Only attacks in which an attacker can spoof trajectory data of a single Smart Vehicle are considered. Trajectory data can, for example, be speed or location. The method is as follows: The authors analyze the I-SIG algorithm and with that identify data spoofing strategies. A vulnerability analysis is conducted to measure the effectiveness

of each data spoofing strategy in a simulator using generic intersection settings. Based on the effectiveness of measures of each data spoofing strategy, the authors perform a cause analysis and construct practical exploits. The practical exploits are evaluated in simulations with real-world intersection settings. The analysis of the I-SIG algorithm shows that (1) *arrival time and phase spoofing* and (2) *queue length manipulation* are viable spoofing strategies. The spoofing strategy (1) can be performed in a full deployment scenario (i.e., when all vehicles are equipped with WAVE) and in transition periods (i.e., periods where a varying percentage of vehicles are equipped with WAVE). As the spoofing strategy (2) is based on adding non-WAVE vehicles to the queue, it can only be performed in transition periods. The consecutive vulnerability analysis shows that the spoofing strategy (1) is capable of increasing delay as high as 68.1%, while the spoofing strategy (2) can increase delay up to 34.6%. The cause for the effectiveness of the spoofing strategy (1) lies in performance optimizations of the signal planning algorithm of I-SIG. These optimizations have been made due to performance limitations on I-SIG RSUs. Both the spoofing strategies (1) and (2) can completely reverse the benefit of the 26.6% decrease in delay when using the I-SIG system. For the simulation with real-world intersection settings the authors craft various exploits that are fine-tuned on the I-SIG algorithm based on the spoofing strategies (1) and (2). The simulations result in increases in delay of up to 181.6% and show that it is even possible to block an entire approach of an intersection. These results reveal that the I-SIG is highly vulnerable to congestion attacks, especially during transition periods. To combat congestion attacks on the I-SIG, the authors suggest to make algorithms more robust against congestion attacks during transition periods, improve the performance of RSUs so that algorithms can be implemented without impeding the security of I-SIG, and employ data spoofing detection using infrastructure-controlled sensors.

Similar attacks may be possible on the TLC service of ETSI C-ITS.

9.2 Vehicular Security

VANET and ETSI C-ITS security focus on secure inter-vehicle communication in the context of a large vehicular network. Classically, however, vehicular security research was based on the security of a limited number of modern vehicles with common components, its in-vehicle communication, and limited remote connectivity (e.g., Miller and Valasek [MV15], Koscher et al. [Kos+10], Nie et al. [Nie+17], Currie [Cur15], Woo et al. [Woo+15], Garcia et al. [Gar+16], Francillon et al. [Fra+11], Alrabady and Mahmud [AM05], or Kulandaivel et al. [Kul+19]). Previously staged attacks in this field have shown the potential impact of attacks on vehicles. In particular cases, security researchers, such as Miller and Valasek [MV15], Koscher et al. [Kos+10], or Nie et al. [Nie+17], were able to exploit vulnerabilities in specific vehicles to control or influence critical systems, such as the steering wheel or the engine. In attacks with malicious intent, such vulnerabilities could easily lead to the death of the vehicle's passengers and people in its proximity. Currie [Cur15] provides a comprehensive timeline of attacks on vehicles between 2010 and 2015.

In current research several papers describe the exploitation of vehicles in a more general manner than Miller and Valasek [MV15] or Koscher et al. [Kos+10] (e.g., Woo et al. [Woo+15] or Miller and Valasek [MV13; MV14]). Woo et al. [Woo+15] discuss a generic approach to perform a long-range wireless attack on a vehicle using a malicious smartphone application. As attacks on vehicles are often costly due to their time-consuming nature and the required expertise, the described attack significantly decreases the costs of attacks. Miller and Valasek [MV13] describe the exploitation of the communication bus in selected vehicles. Such exploits are based on the assumption that it is possible to get remote code execution capabilities on ECUs. It has already been shown in the past that it is possible to get such remote code execution capabilities [Nie+17]. In another paper, Miller and Valasek [MV14] cover remote attack surfaces, internal network architecture, and computer-controlled features. With that, the authors conclude the probability of successful remote attacks on selected vehicles (e.g., the 2014 Jeep Cherokee, the 2014 Audi A8, or the 2014 BMW X3). The authors further discuss strategies to secure vehicles from remote attacks.

A subfield in the field of classical vehicle security is Remote Keyless Entry (RKE), which is based on remote controls [Gar+16]. In this subfield, security researchers have shown multiple times that it is possible to unlock vehicles without possessing a legitimate key, as discussed by Humayed et al. [Hum+17]. Garcia et al. [Gar+16] analyze the Volkswagen (VW) and the Hitag2 RKE systems. The authors show that the corresponding manufacturers VW Group and Next eXPerience Semiconductors (NXP) have used insecure RKE systems for more than 20 years. In both analyzed systems it was possible to clone the original remote control after eavesdropping one or a few lock/unlock actions. Eavesdropping RKE systems is possible with widely available hardware at a low cost.

Passive Keyless Entry and Start (PKES) systems are a special case of RKE systems. PKES systems allow users to unlock and start their vehicles while having their vehicles' keys still in their pocket [Fra+11]. In relay attack on PKES, an attacker that places one antenna near the key holder and a second antenna near the target vehicle can open the target vehicle and start its engine [Fra+11]. Francillon et al. [Fra+11] found that some of the vehicles they tested are vulnerable to relay attacks on their PKES systems. The authors further discuss potential protections against relay attacks, such as checking the key proximity and the usage of multi-channel communication.

Alrabady and Mahmud [AM05] describe the security of RKE systems more generally. The authors aim to support designers of RKE systems with designing their system securely. The authors discuss several attacks on different RKE techniques. Also, the authors propose their own technique. The attacks are categorized according to the difficulty of their execution against RKE techniques and the tools needed for the exploitation of RKE techniques. The authors show that the challenge-response technique and their proposed technique perform well under most attacks.

Kulandaivel et al. [Kul+19] discuss automotive network mapping. The authors argue that in-vehicle networks have become a major target for automotive network attacks

and that automotive network mapping tools are required to understand the security of automotive networks. The authors present such an automotive network mapping tool for the CAN protocol. The tool is called *CANvas*. Testing *CANvas* with a 2009 Toyota Prius and a 2017 Ford Focus, the authors found that network maps for these vehicles can be generated in under an hour.

To ensure safety, the deployment of VANETs arguably requires vehicular security to not only consider traditional vehicular security but to also consider the security of VANETs.

9.3 Blackholing in the Border Gateway Protocol

The BGP is a major routing protocol of the internet [CR05]. In BGP there exists a concept very similar to black hole attacks: blackholing. Nordström and Dovrolis [ND04] describe various BGP attacks, including blackholing. Blackholing makes an IP prefix unreachable from a large portion of the internet. Similarly, black hole attacks on VANETs make ITS stations unreachable through a certain route. Unlike black hole attacks, blackholing can either occur maliciously or non-maliciously. Maliciously, blackholing refers to false route advertisements that attract traffic to a particular router. This router then drops the packets, which results in a DoS. Attracting traffic to a particular router and then dropping the packets is very similar to the two phases of black hole attacks that are described in section 6.1 Black Hole Attacks in Mobile Ad Hoc Networks: absorbing all packets and dropping them. Non-maliciously, blackholing can be used to enforce private and non-allocated IP ranges.

The Secure Path Vector (SPV) protocol by Hu et al. [Hu+04] secures BGP against various attacks, including blackholing. SPV utilizes asymmetric cryptography to extend BGP with integrity. Essentially, SPV protects the Autonomous System PATH (ASPATH) with one-time signatures to prevent malicious truncation and modification of the ASPATH. SPV employs three novel concepts [Hu+04]:

(1) Including private keys within the updates of BGP themselves. [Hu+04]

(2) Not authenticating the autonomous system that inserts itself into the path, but instead employ hop-by-hop authentication. [Hu+04]

(3) Limiting the number of options an attacker has for modifying critical routing information. [Hu+04]

Due to these concepts, SPV has much better performance than similar mechanisms that secure BGP, such as Secure BGP (S-BGP) by Kent et al. [Ken+00]. For example, concept (1) removes the need for a router to store asymmetric private keys. Concept (2) employs one-time signatures based on hash trees so that expensive public-key cryptography can be avoided in cases where performance is critical. [Hu+04]

Caesar and Rexford [CR05] describe BGP routing policies in Internet Service Provider (ISP) networks. The authors point out that blackholing can also be used to block excessive amounts of traffic, as they occur in large-volume DoS attacks. In such a case an ISP would simply drop the DoS traffic destined to the victim. Similarly, an ISP can drop traffic of known spammers. This prevents spammers from establishing bidirectional communication (e.g., with the ISP's mail servers).

Miller et al. [MP19] discuss maliciously used BPG blackholing. The authors describe attacks that combine BGP hijacks with BGP blackholing to novel attacks called BGP blackjacks.

In BGP hijacking, attackers advertise illegitimate routes for IP prefixes they do not own. This illegitimate advertising allows attackers to absorb traffic. Regular BGP hijacks poison the Autonomous Systems (AS') near the attacker. After successful BGP hijacking attackers can, for example, drop packets (i.e., perform blackholing), impersonate the services tied to the hijacked prefix, or eavesdrop traffic.

Similarly, BGP blackjacks poison AS'. In BGP blackjacks an attacker uses BGP blackholing requests to request AS' to blackhole an IP prefix. These blackholing requests take precedence over route advertisements that are used in BPG hijacks. As a result, BGP blackjacks have a potentially higher reach than BGP hijacks. BGP blackjacks are stealthier than BGP hijacks with subsequent blackholing because attackers are not the ones dropping the traffic.

The authors consider the two well-known BGP security mechanisms BGPsec by Lepinski and Sriaram [LS13] and the Resource Public Key Infrastructure (RPKI) protocol by Bush and Austein [BA13] for securing BGP against BGP blackjacks. The authors found that fully-deployed BGPsec provides resistance against most types of BGP blackjacks, while fully-deployed RPKI only provides resistance against BGP blackjacks in certain attack scenarios.

9.4 Mobile Ad Hoc Networks

MANETs are the generic supergroup of VANETs and transitively also the generic supergroup of ETSI C-ITS. As a result, research in MANETs can be, to some extent, applied to VANETs and subsequently to ETSI C-ITS (e.g., Meneguette et al. [Men+18, pp. 28-29], Qu et al. [Qu+15], or Gokhale et al. [Gok+11]). Various aspects of MANETs have been extensively researched in the past (e.g., challenges and applications of MANETs by Goyal et al. [Goy+11] or MANET simulators by Cavin et al. [Cav+02]). Among these aspects are routing protocols and the security of MANETs.

Well-known MANET routing protocols are the AODV protocol [PR99], the OLSR protocol [Cla+03], the DSR protocol [JM96], the TORA protocol [PC97], and the DSDV protocol [PB94].

Research on these protocols has shown their advantages and disadvantages (e.g., Mohseni et al. [Moh+10] or Divecha et al. [Div+07]). In a comparative analysis, Mohseni et

Protocol	Advantages	Disadvantages
AODV	• Adaptive to highly dynamic topologies • Low overhead	• Scalability problems • Large delays
OLSR	• Reduced control overhead and connection	• 2-hop neighbor knowledge required
DSR	• Multiple routes • Loop free • Promiscuous overhead	• Scalability problems • Large delays
TORA	• Multiple routes	• Temporary routing loops • Overall complexity
DSDV	• Loop free	• High overhead

Table 19: Overview of MANET Routing Protocols [Moh+10]

al. [Moh+10] analyzed numerous protocols. Among these protocols were AODV, OLSR, DSR, TORA, and DSDV. The authors describe the advantages and disadvantages of these protocols as in Table 19.

In the early 2000s, Hubaux et al. [Hub+01] and Yang et al. [Yan+04] described the security of MANETs. Hubaux et al. [Hub+01] discusses threats in MANETs. These threats categorize in (1) attacks on the basic mechanisms of MANETs and (2) attacks on security mechanisms. An example of an attack in threat category (1) is possible eavesdropping due to over-the-air communication. An example of an attack in threat category (2) is a possible hijacking of a trusted server. Although the threat categories (1) and (2) are not necessarily specific to MANETs, solutions must consider the specific characteristics of MANETs. The authors neglect the protection of the radio frequency interface, as it is not specific to MANETs. Protections against threat category (1) include tamper resistance of MANET devices and routing-based security mechanisms, protection from the direct neighborhood within the MANET. Protections against threat category (2) focus on the key establishment of cryptographic keys. For that, the authors propose a self-organized public-key infrastructure that is similar to PGP.

Yang et al. [Yan+04] focus on the security of the communication between devices. For this communication, the main threats are (1) attacks on ad hoc routing and (2) attacks on packet forwarding. An example of an attack in threat category (1) is a device that is maliciously advertising itself as an optimal forwarder of packets. An example of an attack in threat category (2) is a device that maliciously drops packets that it is supposed to forward. As protection against the threat categories (1) and (2), the authors propose to use a multi-fence security solution. Such a solution shall be comprised of using different types of routing protocols with security extensions and of employing prevention, detection, and reaction measures. Examples for such measures are the localized detection of misbehaving nodes and the removal of misbehaving nodes from the routing path. Such detection of misbehaving nodes can be done similarly to the misbehavior detection in

VANETs that is described in section 9.6 Misbehavior Detection in Vehicular Ad Hoc Networks.

A more recent description of the security of MANETs has been compiled by Pathan [Pat11]. This work is a summary of various papers in the field of MANETs (e.g., by Guo and Balon [GB06] or by Wex et al. [Wex+08]). The author provides security insights in wireless and self-organizing networks, MANETs, VANETs, WSNs, and WMNs. These security insights consist of security-relevant properties, security challenges, network-specific threats and attacks, and security solutions.

9.5 Performant Cryptographic Algorithms for Vehicular Ad Hoc Networks

As VANETs have critical latency, the overall performance requirements of VANETs are high [Ham+15]. For security, this means cryptographic algorithms should have low computational overhead [Ham+15]. Currently, widely-used cryptographic algorithms, such as the Rivest, Shamir, and Adleman (RSA) algorithm and the Discrete Signature Algorithm (DSA), do not provide optimal performance for VANETs [AP14]. Relatively new Elliptic Curve Cryptography (ECC) based algorithms Elliptic Curve Integrated Encryption Scheme (ECIES) and Elliptic Curve Discrete Signature Algorithm (ECDSA) could substitute RSA and DSA in VANETs [Fer+18].

Both DSRC with WAVE and ETSI specify the usage of ECDSA for digital signatures and the usage of ECIES for asymmetric encryption [Fer+18]. In ETSI C-ITS, ECDSA signatures are used in the ETSI C-ITS security header [Ins17d]. In a performance analysis, Gupta et al. [Gup+02] show that ECDSA strongly outperforms RSA in terms of signature generation with a similar security level. For signature verification, common RSA key lengths, such as 2048 bit, outperform ECDSA with a similar security level. However, with an increasing security level, ECDSA performs increasingly better in signature generation and verification.

Fernandes et al. [Fer+18] discuss the performance of ECDSA with two well-known ECC curves: NIST P-256 and Brainpool P-256. The authors found that the key generation in Brainpool P-256 is much slower than in NIST P-256. For small message sizes, NIST P-256 surpasses Brainpool P-256 in signature verification. However, for larger message sizes, Brainpool P-256 outperforms NIST P-256.

Dai et al. [Dai+17] conduct a performance analysis of ECDSA and ECIES as specified in IEEE 1609.2. Both algorithms meet the performance requirements of DSRC with WAVE for signing/verification and encryption/decryption.

9.6 Misbehavior Detection in Vehicular Ad Hoc Networks

Misbehavior detection can aid in the removal/deactivation of misbehaving ITS stations in ETSI C-ITS. Van der Heijden et al. [Hei+18a] conduct a survey of state-of-the-art

misbehavior detection solutions for VANETs. Misbehavior detection classifies the behavior of entities of a network as correct or incorrect. Correctness refers to whether the entities' behavior reflects the real world or not. Misbehavior detection approaches can be classified into two categories: node-centric and data-centric. In node-centric approaches, knowledge about a sender's messages is used to detect misbehaving entities. This approach can be supported by digital signatures, as they allow to authenticate a sender and, in turn, correlate their messages. Data-centric approaches use the content of messages to determine their correctness. This happens independently from the origin of the message. Typically, data-centric approaches consider data semantics. For example, a data-centric approach would verify the plausibility of movement by analyzing if beacon messages are plausible with respect to the road topology. The authors compare a large number of node-centric and data-centric approaches in terms of scope, resources, generalizability, security, and privacy. This comparison provides an overview of and introduction to the field of misbehavior detection for the industry, developers, standardization agencies, and researchers. As the results of the comparison are very extensive, interested readers are referred to the original paper.

9.7 Traffic Accidents in Traditional Traffic Environments and Vehicular Ad Hoc Networks

VANETs are expected to reduce traffic accidents and related deaths, injuries, and costs all over the world [Mis+16]. Arguably, the security of VANETs influences the rate of traffic accidents. VANETs are used for road safety applications [Men+18, pp. 2-3]. The presence of road safety applications may give drivers of Smart Vehicles a sense of safety. This may lead a driver to rely on road safety applications for their safety in certain situations. If a VANET lacks security and as a result, its road safety application's functionality can be altered or suppressed, a driver could be confused and subsequently be more prone to traffic accidents [Qu+15]. In the worst-case scenario, an attack on VANET's road safety applications can lead to a fatal traffic accident [Qu+15].

In current empiric research, there are multiple cost analyses of traffic accidents in traditional traffic environments (e.g., Kudebong et al. [Kud+11], Mondal et al. [Mon+11], or Rezaei et al. [Rez+14]). As VANETs have only recently started to be deployed [Mis+16], there is no empiric research for traffic accidents in VANETs yet. In the following of this section, multiple cost analyses of traffic accidents in traditional traffic environments are described.

Kudebong et al. [Kud+11] analyzed motorcycle accidents in the capital of the Bolgatanga municipality in Ghana for the year 2008. The authors associate 556 accidents with costs of roughly 1.2 million U.S. dollars.

Mondal et al. [Mon+11] perform an analysis of traffic accidents in India. The authors consider data between 2004 and 2009 and show an increasing number of injuries (~413.900 to ~466.600) and deaths (~91.000 to ~126.000) from traffic accidents during these years.

Rezaei et al. [Rez+14] discuss the extent, consequences, and economic burden of traffic accidents in Iran between March 2009 and March 2010. During this time there were 806.922 related injuries and 22.974 deaths. The authors find that traffic accidents caused costs of about 7.2 billion U.S. dollars.

Naumann et al. [Nau+10] calculate the costs of fatal and non-fatal motor vehicle-related injuries in the U.S. in 2005. These calculations consider total medical costs and lost productivity costs. In total, the costs amount to 99 billion U.S. dollars.

According to the WHO's road safety report [Org15], traffic accidents lead to about 1.24 million deaths per year globally. Considering the current trend of increasing vehicle usage traffic accidents are estimated to become the fifth most common cause of death by 2030.

CHAPTER 10

Findings, Discussion, and Future Work

10.1 Findings on Mobile/Vehicular Ad Hoc Networks and ETSI Cooperative Intelligent Transport Systems

The findings of this thesis can be divided into two parts:

- black hole attacks on MANETs, VANETs, and ETSI C-ITS and
- simulations of black hole attacks in a realistic traffic scenario in ETSI C-ITS.

These findings are described in the following subsections.

10.1.1 Black Hole Attacks on Mobile/Vehicular Ad Hoc Networks and ETSI Cooperative Intelligent Transport Systems

As discussed in section 6.1 Black Hole Attacks in Mobile Ad Hoc Networks, this thesis provides its own definition of black hole attacks in MANETs. This definition aims to be more precise and more complete than other definitions in current research. The proposed definition of a black hole attack is:

> A black hole attack is defined as an attack where one malicious or multiple cooperative malicious nodes
>
> (1) advertise themselves to have an optimal route to a destination for all packets in their communication range in order to absorb the packets and
>
> (2) drop the packets in a way that the packets do not reach their destination.

Subsequently, in subsection 6.1.1 Security-Relevant Properties, this thesis identifies security-relevant properties in MANET routing protocols. These properties are the forwarder selection of the routing protocol, the robustness of the employed routing protocol, the security mechanisms of the employed routing protocol, the attacker/node ratio, the attackers' cooperativeness, the nodes' speed, the attacker proximity, and the safety-criticality of the MANET. The likelihood and impact of black hole attacks in MANETs depend on these properties.

VANETs inherit the security-relevant properties from MANETs. As a particularly security-critical type of MANET, the impact of black hole attacks is relatively high in VANETs. A discussion of performance analyses of black hole attacks in VANET routing protocols shows that performance analyses of MANET routing protocols cannot be used unequivocally to deduct the performance of the same routing protocols in VANETs. A performance analysis employing a realistic traffic scenario by Grimaldo and Martí [GM18] allows assessing the robustness of several well-known MANET/VANET routing protocols in an urban traffic scenario. A definition of the term *realistic traffic scenario* is given in subsection 6.2.1 Robustness of Well-Known Vehicular Ad Hoc Network Routing Protocols. These routing protocols are AODV, DSR, OLSR, and DSDV. AODV is relatively strongly impacted by black hole attacks in the employed scenario. DSDV and OLSR is only slightly impacted overall. The packet delivery ratio of DSR is strongly impacted by the conducted black hole attack.

The robustness analysis of the GeoNetworking protocol in section 7.1 Robustness of the GeoNetworking Protocol finds that GF and CBF can theoretically be attacked with black hole attacks.

The black hole attack scenario on GF discovered in subsection 7.1.2 Greedy Forwarding in GeoUnicast, GeoAnycast, and Simple GeoBroadcast Forwarding is grounded on a lack of authenticity of data that is used in GF. In GF, data of an ITS station's location table is used to forward packets. Without further security measures, this data is not checked for authenticity. As a result, the data can be faked, which allows attackers to effectively spoof an ITS station. An attacker could spoof ITS stations at locations where they would be chosen as optimal forwarders by any genuine sender. Any genuine would send all their GF packets to a spoofed ITS station. These spoofed ITS stations would not forward any packets, which leads to a black hole attack.

The black hole attack scenario on CBF discovered in subsection 7.1.3 Contention-Based Forwarding in GeoUnicast and GeoAnycast is largely based on the inability of genuine ITS stations to reliably distinguish if a packet has been correctly rebroadcasted. In theory, this inability allows attackers to trick genuine ITS stations into incorrectly believing that a packet was rebroadcasted. When these genuine ITS stations are tricked, they refrain from rebroadcasting a packet, leading to a black hole attack. It remains to be shown that the attack on CBF is feasible in practice.

As discussed in section 7.1 Robustness of the GeoNetworking Protocol, black hole attacks on other forwarding algorithms of the GeoNetworking protocol, namely NHBF and

GeoBroadcast forwarding, are not possible. These forwarding algorithms do not employ any packet advertisement mechanism. As a result, in these forwarding algorithms, it is not possible to absorb packets. The impossibility of packet absorption contradicts the necessity of packet absorption in the definition of a black hole attack that is given in section 6.1 Black Hole Attacks in Mobile Ad Hoc Networks.

A subsequent risk analysis following the methodology of ETSI TS 102 165-1 version 4.2.3 [Ins11a] in section 7.5 Risk Analysis of Black Hole Attacks on the GeoNetworking Protocol shows different risks of black hole attacks GF and CBF without security measures and with further security measures. Without security measures and under the presumption that the discovered black hole attack scenario on CBF is feasible in practice, it was found in subsection 7.5.1 Risk without Security Measures that black hole attacks on CBF pose a critical risk to ETSI C-ITS. Black hole attacks on GF also pose a critical risk to ETSI C-ITS, as found in subsection 7.5.1 Risk without Security Measures.

With security measures described in ETSI TR 102 893 [Ins17b] the critical risk of black hole attacks on GF and CBF could be mitigated or even partly prevented, as discussed in subsection 7.5.2 Risk with Vehicle-To-Infrastructure/Infrastructure-To-Vehicle Message Restrictions, subsection 7.5.3 Risk with Detection and Removal/Deactivation of Misbehaving ITS Stations, and subsection 7.5.4 Risk with an Enabled ETSI Cooperative Intelligent Transport Systems Security Header.

As described in subsection 7.5.2 Risk with Vehicle-To-Infrastructure/Infrastructure-To-Vehicle Message Restrictions, *restricting messaging to V2I/I2V communication* would fully prevent the discovered black hole attack scenarios on GF and CBF in areas with ETSI C-ITS infrastructure. However, ETSI C-ITS infrastructure is not expected to be deployed in rural areas in the near future. In areas without ETSI C-ITS infrastructure, messaging can not be restricted to V2I/IV2 communication. As a result, the risk of black hole attacks on GF and CBF would be *none* in areas with ETSI C-ITS infrastructure, but would remain *critical* in areas without ETSI C-ITS infrastructure.

With *the detection and removal/deactivation of misbehaving ITS stations*, ITS stations that cause problems to other ETSI C-ITS stations could be deactivated and/or removed from the routing process, as discussed in subsection 7.5.3 Risk with Detection and Removal/Deactivation of Misbehaving ITS Stations. Detecting and removing/deactivating misbehaving has technical limitations. Detection solutions may not be timely or definitive. These technical limitations allow an attacker to perform the discovered black hole attack scenarios on GF and CBF for a limited time and/or when they are misclassified as not being an attacker. The methodology of ETSI TS 102 165-1 version 4.2.3 [Ins11a] does not factor time limitations or misclassifications. As a result, the risk of black hole attacks on GF and CBF with the security measure of *detection and removal/deactivation misbehaving ITS stations* cannot be evaluated.

Enabling the ETSI C-ITS security header would provide integrity and authenticity to GeoNetworking packets, as discussed in subsection 7.5.4 Risk with an Enabled ETSI Cooperative Intelligent Transport Systems Security Header. The discovered black hole

attack scenario on GF is grounded on a lack of authenticity of data that is used for GF. Enabling the ETSI C-ITS security header would allow genuine ITS stations to check the authenticity of the used data and as a result, fully prevent black hole attacks on GF. However, the discovered black hole attack scenario on CBF is neither based on a lack of integrity or authenticity of packets. *Enabling the ETSI C-ITS security header* would not affect black hole attacks on CBF.

10.1.2 Simulations of Black Hole Attacks in a Realistic Traffic Scenario in ETSI Cooperative Intelligent Transport Systems

Chapter 8 Simulation of Black Hole Attacks in ETSI Cooperative Intelligent Transport Systems describes the selection process of an ETSI-CITS simulation framework that can be extended to allow black hole attack simulations in realistic traffic scenarios. In section 8.2 Selection Process of ETSI Cooperative Intelligent Transport Systems Implementations, it is found that Vanetza is a suitable ETSI C-ITS implementation to enable black hole attack simulations. In section 8.5 Selection Process of Vehicular Ad Hoc Network Simulators, it is discovered that OMNet++ is a fitting VANET simulator. Together Vanetza and OMNet++ constitute an ETSI C-ITS simulation framework. In section 8.7 Development of Black Hole Attack Functionality, important preliminary work is developed to achieve the goal of enabling black hole attacks in ETSI C-ITS. The developed functionality is comprised of enabling to drop GF/CBF packets and to enforce either GF or CBF globally in the selected simulation framework through configuration parameters.

Furthermore, in section 8.8 Data Set with a Realistic Traffic Scenario for Black Hole Attacks, a data set with a realistic and complex traffic scenario is selected for the simulation of black hole attacks in the selected simulation framework. The definition for the term *realistic and complex traffic scenario* is given in subsection 8.8.1 Selection Criteria of Data Sets. It is found that the LuST data set provides a well suited traffic scenario. The integration of the LuST data set into the selected simulation framework is then described together with recommendations for configuring the simulation framework for a realistic and reproducible execution of the traffic scenario. For a realistic and reproducible execution it is important to (1) add a base load of CAM and DENM services and to (2) correctly fix the attacker/Smart Vehicle ratio, the vehicle speed, and the attacker proximity. Task (1) can be done by enabling predefined CAM and DENM services through configuration parameters. Task (2) can be achieved by defining malicious Smart Vehicles and by then configuring an RNG so that it always makes the same Smart Vehicles non-malicious and malicious for every simulation run.

10.2 Discussion of Findings and Outlook on Future Work

Black hole attacks in MANETs are described varyingly in current research (e.g., Tseng et al. [Tse+18], Gokhale et al. [Gok+11], Tamilselvan and Sankaranarayanan [TS07; TS08]). All found descriptions neither aim to be formal nor to be precise or complete. As a result,

these descriptions potentially misrepresent the actual characteristics of black hole attacks. Arguably, research should be based on precise and complete formal definitions to avoid misrepresentation. Future work could assess the formal definition given in this thesis for its precision and completeness or employ its own precise and complete formal definition.

Current research selectively and sometimes inexplicitly cover properties that are relevant for the security of MANETs against black hole attacks. For example, various performance analyses of MANETs under black hole attacks, such as the ones by Bala et al. [Bal+09], by Esmaili et al. [Esm+11], by Ulla and Rehman [UR10], or by Tamilselvan and Sankaranarayan [TS07], do not only show that routing protocols have different robustness against black hole attacks but also indicate that the attacker/node ratio, the attacker cooperativeness, the node speed, and the attacker's proximity to a victim influence the impact of a black hole attack on widely-used routing protocols. Future work in the field of black hole attacks on MANETs should try to identify further security-relevant properties.

In current research many performance analyses of black hole attacks in VANETs are flawed (e.g., Dixit et al. [Dix+16], Saeed et al. [Sae+12], Singh and Agrawal [SA14], Paul et al. [Pau+12], Ahmed et al. [Ahm+14], Kumar et al. [KS19], or Afdhal et al. [Afd+17]), as they do not employ realistic traffic scenarios in accordance to the definition of a *realistic traffic scenario* given in section 6.1 Black Hole Attacks in Mobile Ad Hoc Networks. The performance analysis by Grimaldo and Martí is the first performance analysis employing a realistic traffic scenario that allows deducting the robustness of VANET routing protocols against black hole attacks. Future performance analyses should aim to confirm the results found by Grimaldo and Martí using the same urban traffic scenario or employ a different realistic traffic scenario, possibly in a different area than the analysis by Grimaldo and Martí, such as a highway area or a rural area.

Current research in the field of black hole attacks in VANETs often focuses on well-known routing protocols, such as AODV, DSR, DSDV, or OLSR (e.g., Grimaldo and Martí [GM18], Lachdhaf et al. [Lac+17], Hamid and Mokhtar [HM15], or Purohit et al. [Pur+17]). This research is not directly applicable to the GeoNetworking protocol, as the GeoNetworking protocol differs significantly from AODV, DSR, DSDV, and OLSR. Current research in the field of ETSI C-ITS security frequently covers the overall security of ETSI C-ITS (e.g., Bittl [Bit16] or Kerrache et al. [Ker+16]) or ETSI C-ITS security header-related topics (e.g., Fernandes et al. [Fer+18], Cincilla et al. [Cin+15], Nowdehi [Now13], Nowdehi and Olovsson [NO14], or Haidar et al. [Hai+19]). Presumably, research in black hole attacks on ETSI C-ITS has been neglected so far, since there are several *blind spots* in ETSI C-ITS security research anyways (e.g., flooding attacks, replay attacks, or location disclosure attacks) and there is already extensive research in black hole attacks on VANETs (e.g., Grimaldo and Martí [GM18], Lachdhaf et al. [Lac+17], Hamid and Mokhtar [HM15], or Purohit et al. [Pur+17]). As a result, the robustness analysis of black hole attack on the GeoNetworking protocol in this thesis is the first of its kind.

It is currently not clear with which security measures ETSI C-ITS is deployed initially. As the security measure *ETSI C-ITS security header* is already fully standardized [Ins17d]

it would be reasonable to expect that ETSI C-ITS is initially deployed with an *enabled ETSI C-ITS security header*. As a result, and as discussed in subsection 7.5.4 Risk with an Enabled ETSI Cooperative Intelligent Transport Systems Security Header, users of ETSI C-ITS are protected from black hole attacks on GF, but not from black hole attacks on CBF. The security measures *V2I/I2V message restrictions* and *detection and removal/deactivation of misbehaving ITS stations* are not standardized in ETSI C-ITS. Either these security measures are not planned to be standardized or are not yet standardized. Regardless of that, the lack of standardization hinders the implementation and deployment of these security measures. As a result, it can be expected that neither *V2I/I2V message restrictions* nor *detection and removal/deactivation of misbehaving ITS stations* are functional during the initial deployment of ETSI C-ITS. Instead, these security measures might be introduced at a later time. Until then, users of ETSI C-ITS will be susceptible to black hole attacks on CBF. As discussed in subsection 7.5.2 Risk with Vehicle-To-Infrastructure/Infrastructure-To-Vehicle Message Restrictions, after the enforcement of *V2I/I2V message restrictions*, users of ETSI C-ITS will be protected from black hole attacks on GF and CBF wherever ETSI C-ITS infrastructure is in place. After the deployment of *detection and removal/deactivation of misbehaving ITS stations*, users of ETSI C-ITS will be protected from black hole attacks on GF and CBF except for the time it takes a misbehavior detection to detect black hole attacks and except for misclassifications, as discussed in subsection 7.5.4 Risk with an Enabled ETSI Cooperative Intelligent Transport Systems Security Header. The protection from black hole attacks on GF due to *V2I/I2V message restrictions* and *detection and removal/deactivation of misbehaving ITS stations* adds to the protection provided by an enabled ETSI C-ITS security header.

Another potential solution to prevent black hole attacks in ETSI C-ITS would be (1) the introduction of security mechanisms in GF and CBF, similar to the introduction of security mechanisms into AODV by Tamilselvan and Sankaranarayan [TS07; TS08] and Ramaswamy et al. [Ram+03], or (2) the standardization of AODV with security mechanisms in ETSI C-ITS. However, as GF and CBF are designed with specific advantages (e.g., the robustness to connection errors of CBF or the good performance of GF), it is unlikely that solution (2) alone could replace GF and CBF without major drawbacks.

There may be more black hole attack scenarios possible on the GeoNetworking protocol than found in this thesis. Future work should not only aim to confirm the discovered black hole attack scenarios in theory and practice, but also aim to find further black hole attack scenarios on the GeoNetworking protocol. The GeoNetworking protocol may also be at risk of attacks similar to black hole attacks. The GeoNetworking protocol is based on geographic positions of ITS stations [Ins17a]. ITS stations obtain location information through GNSS [Ins12b], which can be faked, as shown by Papadimitratos and Jovanovic [PJ08]. Such faking may allow an attacker to perform large-scale DoS by exploiting the location-based forwarding of the GeoNetworking protocol. For example, ITS stations may be tricked into believing they are not in the geographic target area of a GeoBroadcast packet, even if they are. According to the behavior of GeoBroadcast

given in subsection 4.3.2 GeoNetworking, this would lead the ITS station to forward the packet via GeoUnicast instead of broadcasting it.

Both the risk analysis in this thesis and the TVRA of ETSI TR 102 893 [Ins17b] follow the risk analysis method of ETSI TS 102 165-1 version 4.2.3 [Ins11a]. However, the TVRA analyzes black hole attacks in less detail than the security analysis in this thesis. Particularly, the TVRA analyzes black hole attacks in larger threat groups. Unlike the risk analysis in this thesis, the TVRA does not separately analyze the risk of black hole attacks on individual forwarding algorithms of the GeoNetworking protocol. As a result, the risk analysis in this thesis provides more detailed information on the risk of black hole attacks on ETSI C-ITS than the TVRA. Similarly, future work could choose threats and/or security measures from the TVRA and provide more in-depth information on these threats/security measures. For example, misbehavior detection is described relatively superficial in the TVRA and could be analyzed in more detail for ETSI C-ITS in future work.

Currently, no well-known open-source ETSI C-ITS implementation allows simulations of black hole attacks. The functionality developed in this thesis brings simulations in such implementations closer to being possible. Future work should continue to work on enabling black hole attack simulations in ETSI C-ITS implementations. As soon as black hole attacks can be simulated, future work can conduct performance analyses of individual GeoNeworking forwarding algorithms under black hole attacks and the security of the GeoNetworking Protocol against Black Hole Attacks.

For simulations to accurately reflect the real world and be generally applicable, realistic and complex traffic scenarios need to be used in future work [Cod+17]. Codeca et al. [Cod+17], Codeca and Härri [CH18], and the SUMO Website [Cen] discuss the level of realism of several data sets that employ complex traffic scenarios (e.g., the Bologna Ringway data set, the TAPAS Cologne data set, or the LuST data set). Among the data set selected for this thesis, namely the LuST data set, there is another promising candidate for simulating realistic and complex traffic scenarios in the selected simulation framework: the MoST data set. However, integrating the MoST data set into the selection simulation framework leads to failing timing assertions. As a result, the MoST data set could not be used in this thesis. If this problem was fixed in future work, the MoST data set would be even better suited than the LuST data set.

CHAPTER 11

Conclusion

In this thesis, a precise and complete formal definition of black hole attacks in MANETs/VANETs was given. Subsequently, several properties relevant to the security of black hole attacks on MANETs/VANETs were identified.

A robustness analysis was conducted to theoretically assess the robustness of the GeoNetworking protocol against black hole attacks. During this robustness analysis two black hole attack scenarios were discovered. One black hole attack scenario can be used to attack GF, the other can be used to attack CBF. The later risk analysis showed that the risk of these attacks is critical to ETSI C-ITS without further security measures. The security measure *ETSI C-ITS security header* is likely to be enabled during the initial deployment of ETSI C-ITS. As a result, users of ETSI C-ITS are protected from black hole attacks on GF. However, the security measures *V2I/I2V message restrictions* and *detection and removal/deactivation of misbehaving ITS stations* will likely not be available during initial deployment. Instead, they will likely be deployed at a later time. Until then, users of ETSI C-ITS will be susceptible to black hole attacks on CBF. After the enforcement of *V2I/I2V message restrictions*, users of ETSI C-ITS will be protected from black hole attacks on CBF wherever ETSI C-ITS infrastructure is available. After the deployment of *detection and removal/deactivation of misbehaving ITS stations*, users of ETSI C-ITS will be protected from black hole attacks on CBF except for the time it takes a misbehavior detection solution to detect black hole attacks and except for misclassifications.

The ETSI C-ITS implementation Vanetza, the packet-level simulator OMNet++, and the LuST data set were combined to have a simulation framework with a realistic and complex traffic scenario. For the simulation framework, black hole attack functionality was developed. The developed functionality is comprised of functionality to drop GF and CBF packets and functionality to enforce either GF or CBF globally.

List of Figures

List of Tables

List of Acronyms

3GPP Third Generation Partnership Project

5G 5th Generation of Cellular Networks

AA Authorization Authority

ACPN A Novel Framework with Conditional Privacy-Preservation and Non-Repudiation

AES Advanced Encryption Standard

AODV Ad Hoc On-Demand Distance Vector

ART Attack-Resistant Trust

ASPATH Autonomous System Path

AT Authorization Ticket

BC Bootstrap Certificate

BGP Border Gateway Protocol

BTP Basic Transport Protocol

C-ITS Cooperative Intelligent Transport Systems

CA Certificate Authority

CALM Communication Access for Land Mobiles

CAM Cooperative Awareness Message

CAN Controller Area Network

CBF Contention-Based Forwarding

CCA Chosen Ciphertext Attack

CCA2 Adaptive Chosen Ciphertext Attack

CCH Control Channel

CDMA Code Division Multiple Access

CEN Comité Européen de Normalisation

CIA Triad Confidentiality, Integrity, and Availability Triad

CPA Chosen Plaintext Attack

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

DC$^+$-net Improved Dining Cryptographers Network

DC-net Dining Cryptographers Network

DCC Decentralized Congestion Control

DDoS Distributed Denial-of-Service

DENM Distributed Environmental Notification Message

DoS Denial-of-Service

DSA Discrete Signature Algorithm

DSRC Dedicated Short-Range Communciation

EA Enrollment Authority

EC Enrollment Credential

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Discrete Signature Algorithm

ECIES Elliptic Curve Integrated Encryption Scheme

ECU Electronic Control Unit

EDCA Enhanced Distributed Coordination Access

ETSI European Telecommunications Standards Institute

GBF GeoBroadcast Forwarding

GF Greedy Forwarding

GN6 Geonetworking via IPv6

GNSS Global Navigation Satellite System

GPC GNSS Positioning Correction

GPSR Greedy Perimeter Stateless Routing

GyTAR Greedy Traffic Aware Routing

I-SIG Intelligent Traffic Signal System

I2V Infrastructure-to-Vehicle

ICRW Intersection Collision Risk Warning

IEEE Institute of Electrical and Electronics Engineers

IND Indistinguishability

IND-CCA Indistinguishability under a Chosen Ciphertext Attack

IND-CCA2 Indistinguishability under an Adaptive Chosen Ciphertext Attack

IND-CPA Indistinguishability under a Chosen Plaintext Attack

IP Internet Protocol

IPv6 IP version 6

ISO International Organization for Standardization

ISP Internet Service Provider

ITS Intelligent Transport Systems

ITS-G5 Intelligent Transport Systems 5 GHz

ITS-G5A Band A of ITS-G5

ITS-G5B Band B of ITS-G5

ITS-G5C Band C of ITS-G5

ITS-G5D Band D of ITS-G5

IVI Infrastructure-to-Vehicle Information

IVIM Infrastructure-to-Vehicle Message

KDC Key Distribution Center

LCRW Longitudinal Collision Risk Warning

LIN Local Interconnect Network

LLC Logical Link Control

LS Location Service

LTE Long-Term Evolution

LuST Luxembourg SUMO Traffic

MAC Media Access Control

MAC Message Authentication Code

MANET Mobile Ad Hoc Network

MAPEM MAP Extended Message

MCTP Mobile Control Transport Protocol

MDA Minimum Dissemination Area

MFR Most Forward within Radius

MIB Management Information Base

MoST Monaco SUMO Traffic

MULTOPS MUlti-Level Tree for Online Packet Statistics

NHBF N-Hop Broadcast Forwarding

NIST National Institute of Standards and Technology

NISTIR National Institute of Standards and Technology Interagency/Internal Report

NM Non-Malleability

NM-CCA Non-Malleability under a Chosen Ciphertext Attack

NM-CCA2 Non-Malleability under an Adaptive Chosen Ciphertext Attack

NM-CPA Non-Malleability under a Chosen Plaintext Attack

NS-3 Network Simulator 3

NXP Next eXPerience Semiconductors

OBU On-Board Unit

OMNet++ Objective Modular Network Testbed in C++

OSI Open Systems Interconnection

PACP Pseudonymous Authentication-Based Conditional Privacy

PGP Pretty Good Privacy

PHY Physical Layer of ETSI C-ITS

PICS Protocol Implementation Conformance Statement

PIXIT Protocol Implementation eXtra Information for Testing

PKES Passive Keyless Entry and Start

PKI Public Key Infrastructure

QoS Quality of Service

RC4 Ron's Code 4

RHS Road Hazard Signalling

RKE Remote Keyless Entry

RLAN Radio Local Area Network

RLT Road Lane Topology

RNG Random Number Generator

RPKI Resource Public Key Infrastructure

RSA Rivest, Shamir, and Adleman

RTCM Radio Technical Commission for Maritime Services

RTCMEM Radio Technical Commission for Maritime Services Extended Message

S-BGP Secure Border Gateway Protocol

SCF Store-Carry-Forward

SCH Service Channel

SDMA Space Division Multiple Access

SHB Single-Hop Broadcast

SPAT Signal Phase and Time

SPATEM Signal Phase and Time Extended Mssage

SPV Secure Path Vector

SREM Signal Request Extended Message

SSEM Signal Request Status Extended Message

SUMO Simulation of Urban MObility

TAPAS Travel and Activity PAtterns Simulation

TCP Transport Control Protocol

TDMA Time Division Multiple Access

TLC Traffic Light Control

TLM Traffic Light Maneuver

TR Technical Report

TS Technical Specification

TSB Topologically Scoped Broadcast

TVRA Threat, Vulnerability, and Risk Analysis

UDP User Datagram Protocol

V-TRADE Vectorbased TRAcking DEtection

V2I Vehicle-to-Infrastructure

V2V Vehicle-to-Vehicle

V2X Vehicle-to-Anything

VANET Vehicular Ad Hoc Network

VTP Vehicle Transport Protocol

VW Volkswagen

WAVE Wireless Access in Vehicular Environments

WLAN Wireless Local Area Network

Bibliography

[Afd+17] Afdhal et al. “Black hole attacks analysis for AODV and AOMDV routing performance in VANETs”. In: *International Conference on Electrical Engineering and Informatics*. (2017).

[Ahm+14] Ahmed et al. “Performance evaluation of black hole attack on VANETs’ routing protocols”. In: *International Journal of Software Engineering and its Applications*. (2014).

[AM05] Alrabady and Mahmud. “Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs”. In: *IEEE Transactions on Vehicular Technology*. (2005).

[Amo+15] Amoozadeh et al. “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving”. In: *IEEE Communications Magazine*. (2015).

[AP14] Alimohammadi and Pouyan. “Performance analysis of cryptography methods for secure message exchanging in VANET”. In: *International Journal of Scientific & Engineering Research*. (2014).

[Ars+18] Arshad et al. “A survey of local/cooperative-based malicious information detection techniques in VANETs”. In: *EURASIP Journal on Wireless Communications and Networking*. (2018).

[Aut+13] Autolitano et al. “An insight into DCC techniques for VANETs from ETSI TS 102 687 V1.1.1”. In: *IFIP Wireless Days*. (2013).

[AW10] Arbabi and Weigle. “Highway mobility and VANETs in NS-3”. In: *Proceedings of the Winter Simulation Conference*. (2010).

[BA13] Bush and Austein. *RFC 6810: The resource public key infrastructure to router protocol*. (2013).

[Bai+16] Baiad et al. “Novel cross layer detection schemes to detect black hole attack against QoS-OLSR protocol in VANETs”. In: *Vehicular Communications*. (2016).

[Bal+09] Bala et al. “Performance analysis of MANETs under black hole attacks”. In: *1st International Conference on Networks and Communications*. (2009).

[Bec+05] Bechler et al. “An optimized TCP for internet access of VANETs”. In: *International Conference on Research in Networking*. (2005).

[Bel+98] Bellare et al. “Relations among notions of security for public-key encryption schemes”. In: *Annual International Cryptology Conference*. (1998).

[Ber08] Bernstein. “ChaCha, a variant of Salsa20”. In: *Workshop Record of SASC*. (2008).

[Bib+12] Bibhu et al. “Performance analysis of black hole attack in VANET”. In: *International Journal of Computer Network and Information Security*. (2012).

[Bis09] Biskup. *Security in computing systems: Challenges, approaches, and solutions*. Springer Berlin Heidelberg, 2009. ISBN: 978-3-540-78441-8.

[Bit16] Sebastian Bittl. “Towards solutions for current security-related issues in ETSI C-ITS”. In: *International Workshop on Communication Technologies for Vehicles*. (2016).

[Bit17] Bittl. “Efficient secure communication in VANETs under the presence of new requirements emerging from advanced attacks”. PhD thesis. Humboldt-Universität zu Berlin, 2017.

[BN00] Bellare and Namprempre. “Authenticated encryption: Relations among notions and analysis of the generic composition paradigm”. In: *Advances in Cryptology*. (2000).

[Bor+01] Borisov et al. “Intercepting mobile communications: The insecurity of 802.11”. In: *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*. (2001).

[Bur+08] Burmester et al. “Strengthening privacy protection in VANETs”. In: *IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications*. (2008).

[Cal+07] Calandriello et al. “Efficient and robust pseudonymous authentication in VANETs”. In: *Proceedings of the 4th ACM International Workshop on VANETs*. (2007).

[Cav+02] Cavin et al. “On the accuracy of MANET simulators”. In: *Proceedings of the 2nd ACM International Workshop on Principles of Mobile Computing*. (2002).

[CB95] Cooper and Birman. “Preserving privacy in a network of mobile computers”. In: *Proceedings 1995 IEEE Symposium on Security and Privacy*. (1995).

[CE14] Chen and Englund. “Cooperative ITS – EU standards to accelerate cooperative mobility”. In: *International Conference on Connected Vehicles*. (2014).

[CH18] Codecá and Härri. “Monaco SUMO Traffic scenario: A 3D mobility scenario for cooperative ITS”. In: *SUMO User Conference: Simulating Autonomous and Intermodal Transport Systems*. (2018).

[Cha16] Chaubey. “Security analysis of VANETs: A comprehensive study”. In: *International Journal of Security and Its Applications.* (2016).

[Cha81] Chaum. “Untraceable electronic mail, return addresses and digital pseudonyms”. In: *Secure Electronic Voting.* (1981).

[Cha85] Chaum. “Security without identification: Transaction systems to make big brother obsolete”. In: *Communications of the ACM.* (1985).

[Cha88] Chaum. “The dining cryptographers problem: Unconditional sender and recipient untraceability”. In: *Journal of Cryptology.* (1988).

[Che+18] Chen et al. “Exposing congestion attack on emerging connected vehicle based traffic signal control.” In: *Network and Distributed System Security Symposium.* (2018).

[Cin+15] Cincilla et al. “Security of C-ITS messages: A practical solution the ISE project demonstrator”. In: *7th International Conference on New Technologies, Mobility and Security.* (2015).

[CK01] Canetti and Krawczyk. “Analysis of key-exchange protocols and their use for building secure channels”. In: *International Conference on the Theory and Applications of Cryptographic Techniques.* (2001).

[Cla+03] Clausen et al. *Optimized link state routing protocol.* 2003.

[Cod+17] Codecá et al. “Luxembourg SUMO traffic scenario: Traffic demand evaluation”. In: *IEEE ITS Magazine.* (2017).

[Coo+08] Cooper et al. *RFC 5280: Internet X. 509 public key infrastructure certificate and certificate revocation list profile.* (2008).

[CR05] Caesar and Rexford. “BGP routing policies in ISP networks”. In: *IEEE Network.* (2005).

[Cun+16] Da Cunha et al. “Data communication in VANETs: Protocols, applications and challenges”. In: *Ad Hoc Networks.* (2016).

[CZ10] Chowdhury and Zulkernine. “Can complexity, coupling, and cohesion metrics be used as early indicators of vulnerabilities?” In: *Proceedings of the ACM Symposium on Applied Computing.* (2010).

[Dai+17] Dai et al. “The implementation and performance evaluation of wave-based secured vehicular communication system”. In: *IEEE 85th Vehicular Technology Conference.* (2017).

[Dan+14] Dang et al. “HER-MAC: A hybrid efficient and reliable MAC for vehicular ad hoc networks”. In: *IEEE 28th International Conference on Advanced Information Networking and Applications.* (2014).

[DB05] Desilva and Boppana. “Mitigating malicious control packet floods in ad hoc networks”. In: *IEEE Wireless Communications and Networking Conference.* (2005).

[Den+02] Deng et al. “Routing security in wireless ad hoc networks.” In: *IEEE Communications Magazine.* (2002).

[DH17] Deering and Hinden. *RFC 8200: IPv6 specification.* (2017).

[Dia+02] Diaz et al. “Towards measuring anonymity”. In: *International Workshop on Privacy Enhancing Technologies.* (2002).

[Div+07] Divecha et al. “Impact of node mobility on MANET routing protocol models.” In: *Journal of Digital Information Management* (2007).

[Dix+16] Dixit et al. “VANET: Architectures, research issues, routing protocols, and its applications”. In: *International Conference on Computing, Communication, and Automation.* (2016).

[DN92] Dwork and Naor. “Pricing via processing or combatting junk mail”. In: *Advances in Cryptology.* (1992).

[Dol+91] Dolev et al. “Non-malleable cryptography”. In: *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing.* (1991).

[DR99] Daemen and Rijmen. *AES proposal: Rijndael.* (1999).

[DZ83] Day and Zimmermann. “The OSI reference model”. In: *Proceedings of the IEEE.* (1983).

[Eng+14] Engoulou et al. “VANET security surveys”. In: *Computer Communications.* (2014).

[Esm+11] Esmaili et al. “Performance analysis of AODV under black hole attacks through use of the OPNET simulator”. In: *arXiv Preprint arXiv:1104.4544.* (2011).

[Fü+04] Füßler et al. “Contention-based forwarding for street scenarios”. In: *1st International Workshop in Intelligent Transportation.* (2004).

[Fer+18] Fernandes et al. “Implementation and analysis of IEEE and ETSI security standards for vehicular communication”. In: *Mobile Networks and Applications.* (2018).

[Fes14] Festag. “C-ITS standards in Europe”. In: *IEEE Communications Magazine.* (2014).

[Fes15] Festag. “Standards for vehicular communication—from IEEE 802.11 p to 5G”. In: *Elektrotechnik und Informationstechnik.* (2015).

[FR11] Farwell and Rohozinski. “Stuxnet and the future of cyber war”. In: *Survival.* (2011).

[Fra+11] Francillon et al. “Relay attacks on passive keyless entry and start systems in modern cars”. In: *Proceedings of the Network and Distributed System Security Symposium.* (2011).

[Füß+03] Füßler et al. “Contention-based forwarding for MANETs”. In: *Ad Hoc Networks.* (2003).

[Gal85] Gallager. “A perspective on multiaccess channels”. In: *IEEE Transactions on Information Theory*. (1985).

[Gam00] Gambetta. “Can we trust trust”. In: *Trust: Making and Breaking Cooperative Relations*. (2000).

[Gar+16] Garcia et al. “Lock it and still lose it – On the (in)security of automotive remote keyless entry systems”. In: *25th USENIX Security Symposium*. (2016).

[Gar95] Garfinkel. *PGP: pretty good privacy*. O’Reilly Media Inc., 1995. ISBN: 978-1-565-92098-9.

[GB06] Guo and Balon. *VANETs and DSRC*. 2006.

[Gil+15] Gillani et al. “MAC layer challenges and proposed protocols for vehicular ad hoc networks”. In: *Vehicular Ad Hoc Networks for Smart Cities*. (2015).

[Gla+11] Glass et al. “Securing route and path integrity in multi-hop wireless networks”. In: *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC Press, 2011. ISBN: 978-1-4398-1920-3.

[GM18] Grimaldo and Martí. “Performance comparison of routing protocols in VANETs under black hole attacks in Panama City”. In: *International Conference on Electronics, Communications, and Computers*. (2018).

[GM84] Goldwasser and Micali. “Probabilistic encryption”. In: *Journal of Computer and System Sciences*. (1984).

[Gok+11] Gokhale et al. “Classification of attacks on wireless MANETs and VANETs – A Survey”. In: *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC Press, 2011. ISBN: 978-1-4398-1920-3.

[Goy+11] Goyal et al. “MANET: Vulnerabilities, challenges, attacks, and application”. In: *International Journal of Computational Engineering & Management*. (2011).

[Goz+09] Gozalvez et al. “iTETRIS: the framework for large-scale research on the impact of cooperative wireless vehicular communications systems in traffic efficiency”. In: *Information and Communications Technologies*. (2009).

[GP01] Gil and Poletto. “MULTOPS: A data-structure for bandwidth attack detection.” In: *USENIX Security Symposium*. (2001).

[GP09] Golle and Partridge. “On the anonymity of home/work location pairs”. In: *International Conference on Pervasive Computing*. (2009).

[Gro+11] Grover et al. “Sybil attacks in VANETs”. In: *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC Press, 2011. ISBN: 978-1-4398-1920-3.

[Gro16] DSRC Working Group. *IEEE standard for wireless access in vehicular environments—security services for applications and management messages*. (2016).

[Gün+17] Güneş et al. *MANET protocols based on dissimilarity metrics*. Springer, 2017. ISBN: 978-3-319-62739-7.

[Gup+02] Gupta et al. "Performance analysis of ECC for SSL". In: *Proceedings of the 1st ACM Workshop on Wireless Security*. (2002).

[Hai+19] Haidar et al. "Risk analysis on C-ITS pseudonymity aspects". In: *10th IFIP International Conference on New Technologies, Mobility, and Security*. (2019).

[Ham+15] Hamida et al. "Security of C-ITS: Standards, threats analysis and cryptographic countermeasures". In: *Electronics*. (2015).

[Has+17] Hasrouny et al. "VANET security challenges and solutions: A survey". In: *Vehicular Communications*. (2017).

[Hei+18a] Van der Heijden et al. "Survey on misbehavior detection in C-ITS". In: *IEEE Communications Surveys and Tutorials*. (2018).

[Hei+18b] Van der Heijden et al. "VeReMi: A dataset for comparable evaluation of misbehavior detection in VANETs". In: *Security and Privacy in Communication Networks*. (2018).

[HM15] Hamid and Mokhtar. "Performance analysis of the VANET routing protocols AODV, DSDV and OLSR". In: *5th International Conference on Information Technology, Communication Technology, and Accessibility*. (2015).

[Hu+04] Hu et al. "SPV: Secure path vector routing for securing BGP". In: *ACM SIGCOMM Computer Communication Review*. (2004).

[Hu+17] Hu et al. "REPLACE: A reliable trust-based platoon service recommendation scheme in VANETs". In: *IEEE Transactions on Vehicular Technology*. (2017).

[Hua+06] Huanguo et al. "Development of trusted computing research". In: *Wuhan University Journal of Natural Sciences*. (2006).

[Hua+11] Huang et al. "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs". In: *IEEE Transactions on ITS*. (2011).

[Hub+01] Hubaux et al. "The quest for security in MANETs". In: *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing*. (2001).

[Hum+17] Humayed et al. "Cyber-physical systems security: A survey". In: *IEEE Internet of Things Journal*. (2017).

[Ins03] European Telecommunications Standards Institute. *ETSI TS 102 165-1 V4.1.1 - CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)*. (2003).

[Ins09] European Telecommunications Standards Institute. *ETSI TR 102 638 V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. (2009).

[Ins10a] European Telecommunications Standards Institute. *ETSI EN 202 663 V1.1.0 - Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band.* (2010).

[Ins10b] European Telecommunications Standards Institute. *ETSI EN 302 665 V1.1.1 - Intelligent Transport Systems (ITS);Communications Architecture.* (2010).

[Ins10c] European Telecommunications Standards Institute. *ETSI TS 102 941 V1.2.1 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.* (2010).

[Ins11a] European Telecommunications Standards Institute. *ETSI TS 102 165-1 V4.2.3 - CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA).* (2011).

[Ins11b] European Telecommunications Standards Institute. *ETSI TS 102 636-4-1 V.1.1 - Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality.* (2011).

[Ins12a] European Telecommunications Standards Institute. *ETSI TR 102 861 V1.1.1 - Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part.* (2012).

[Ins12b] European Telecommunications Standards Institute. *ETSI TS 102 724 V1.1.1 - Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band.* (2012).

[Ins12c] European Telecommunications Standards Institute. *ETSI TS 102 942 V1.1.1 - Intelligent Transport Systems (ITS); Security; Access Control.* (2012).

[Ins12d] European Telecommunications Standards Institute. *ETSI TS 102 943 V1.1.1 - Intelligent Transport Systems (ITS); Security; Confidentiality services.* (2012).

[Ins13a] European Telecommunications Standards Institute. *ETSI EN 302 636-2 V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Geonetworking; Part 2: Scenarios.* (2013).

[Ins13b] European Telecommunications Standards Institute. *ETSI TR 101 607 V1.1.1 - Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1.* (2013).

[Ins13c] European Telecommunications Standards Institute. *ETSI TS 101 539-1 V1.1.1 - Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification.* (2013).

[Ins13d] European Telecommunications Standards Institute. *ETSI TS 101 539-3 V1.1.1 - Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification.* (2013).

[Ins14a] European Telecommunications Standards Institute. *ETSI EN 302 636-1 – Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements.* (2014).

[Ins14b] European Telecommunications Standards Institute. *ETSI EN 302 636-3 – Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture.* (2014).

[Ins14c] European Telecommunications Standards Institute. *ETSI EN 303 613 V1.1.1 – Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols.* (2014).

[Ins14d] European Telecommunications Standards Institute. *ETSI TS 302 636-5-1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol.* (2014).

[Ins15] European Telecommunications Standards Institute. *ETSI TS 103 175 V1.1.1 - Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium.* (2015).

[Ins17a] European Telecommunications Standards Institute. *ETSI EN 302 636-4-1 V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality.* (2017).

[Ins17b] European Telecommunications Standards Institute. *ETSI TR 102 893 - Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA).* (2017).

[Ins17c] European Telecommunications Standards Institute. *ETSI TS 102 165-1 V5.2.3 - CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA).* (2017).

[Ins17d] European Telecommunications Standards Institute. *ETSI TS 103 097 V1.3.1 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats.* (2017).

[Ins18a] European Telecommunications Standards Institute. *ETSI TS 101 539-2 V1.1.1 - Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification.* (2018).

[Ins18b] European Telecommunications Standards Institute. *ETSI TS 102 940 V1.3.1 - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.* (2018).

[Ins18c] European Telecommunications Standards Institute. *ETSI TS 103 301 V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services.* (2018).

[Ins18d] European Telecommunications Standards Institute. *TS 102 687 V1.2.1 – Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part.* (2018).

[Ins19] European Telecommunications Standards Institute. *ETSI EN 302 663 V1.3.1 - Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.* (2019).

[Ins20] European Telecommunications Standards Institute. *ETSI EN 303 613 V1.1.1 - Intelligent Transport Systems (ITS); LTE-V2X access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.* (2020).

[Jay11] Jaydip. "Reputation-and trust-based systems for wireless self-organizing networks". In: *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC Press, 2011. ISBN: 978-1-4398-1920-3.

[Jer+07] Jerbi et al. "An improved vehicular ad hoc routing protocol for city environments". In: *IEEE International Conference on Communications.* (2007).

[JM96] Johnson and Maltz. "Dynamic source routing in ad hoc wireless networks". In: *Mobile Computing.* (1996).

[Kal+13] Kale et al. "An overview of MANETs". In: *International journal of computer science and applications.* (2013).

[KD11] Kumar and Dave. "A comparative study of various routing protocols in VANET". In: *arXiv preprint arXiv:1108.2094.* (2011).

[Ken+00] Kent et al. "Secure border gateway protocol". In: *IEEE Journal on Selected Areas in Communications.* (2000).

[Ken11] Kenney. "DSRC standards in the United States". In: *Proceedings of the IEEE.* (2011).

[Ker+16] Kerrache et al. "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS". In: *Computer Communications.* (2016).

[KK00] Karp and Kung. "GPSR: Greedy perimeter stateless routing for wireless networks." In: *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking.* (2000).

[KK15] Kaiwartya and Kumar. “Cache agent-based geocasting in VANETs”. In: *International Journal of Information and Communication Technology*. (2015).

[KL14] Katz and Lindell. *Introduction to modern cryptography*. CRC press, 2014. ISBN: 978-1-4665-7027-6.

[Kos+10] Koscher et al. “Experimental security analysis of a modern automobile”. In: *IEEE Symposium on Security and Privacy*. (2010).

[KP16] Khodaei and Papadimitratos. “Evaluating on-demand pseudonym acquisition policies in vehicular communication systems”. In: *Proceedings of the 1st International Workshop on Internet of Vehicles and Vehicles of Internet*. (2016).

[Kra+97] Krauß et al. “Metastable states in a microscopic model of traffic flow”. In: *Physical Review*. (1997).

[KS19] Kumar and Sinha. “Design and analysis of an improved AODV protocol for black hole and flooding attacks in VANETs”. In: *Journal of Discrete Mathematical Sciences and Cryptography*. (2019).

[Kub+16] Kubička et al. “Performance of current eco-routing methods”. In: *IEEE Intelligent Vehicles Symposium*. (2016).

[Kud+11] Kudebong et al. “Economic burden of motorcycle accidents in Northern Ghana”. In: *Ghana Medical Journal*. (2011).

[Kul+19] Kulandaivel et al. “CANvas: Fast and inexpensive automotive network mapping”. In: *28th USENIX Security Symposium*. (2019).

[Lac+17] Lachdhaf et al. “Detection and prevention of black hole attacks in VANETs using secured AODV Routing Protocol”. In: *International Conference on Networks and Communications*. (2017).

[Lan01] Landwehr. “Computer security”. In: *International Journal of Information Security*. (2001).

[Lau+16] Laux et al. “Demo: OpenC2X – An open source experimental and prototyping platform supporting ETSI ITS-G5”. In: *IEEE Vehicular Networking Conference*. (2016).

[Law+13] Lawrenz et al. *CAN System Engineering*. Springer, 2013. ISBN: 978-1-4471-5613-0.

[LB06] Laurendeau and Barbeau. “Threats to security in DSRC/WAVE”. In: *International Conference on Ad Hoc Networks and Wireless*. (2006).

[LC16] Lonc and Cincilla. “C-ITS security framework: Standards and implementations progress in Europe”. In: *IEEE 17th International Symposium on A World of Wireless, Mobile, and Multimedia Networks*. (2016).

[Li10] Li. “An overview of the DSRC/WAVE technology”. In: *International Conference on Heterogeneous Networking for Quality, Reliability, Security, and Robustness*. (2010).

[Li+14] Li et al. “ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs”. In: *IEEE Transactions on Parallel and Distributed Systems*. (2014).

[Liu+15] Liu et al. “A software defined network architecture for geobroadcast in VANETs”. In: *IEEE International Conference on Communications*. (2015).

[LL15] Lin and Lu. *VANET security and privacy*. John Wiley & Sons, 2015. ISBN: 978-1-118-91390-1.

[Lla+15] Llatser et al. “Greedy algorithms for information dissemination within groups of autonomous vehicles”. In: *IEEE Intelligent Vehicles Symposium*. (2015).

[LS01a] Liu and Singh. “ATCP: TCP for mobile ad hoc networks”. In: *IEEE Journal on Selected Areas in Communications*. (2001).

[LS01b] Loscocco and Smalley. “Integrating flexible support for security policies into the Linux operating system.” In: *USENIX Annual Technical Conference*. (2001).

[LS13] Lepinski and Sriram. *RFC 8205: BGPSEC protocol specification*. (2013).

[LS16] Li and Song. “ART: An attack-resistant trust management scheme for securing VANET”. In: *IEEE Transactions on ITS*. (2016).

[Lu+14] Lu et al. “Connected vehicles: Solutions and challenges”. In: *IEEE Internet of Things Journal*. (2014).

[LV89] Lupas and Verdu. “Linear multi-user detectors for synchronous CDMA channels”. In: *IEEE Transactions on Information Theory*. (1989).

[MA15] Mokhtar and Azab. “Survey on security issues in VANETs”. In: *Alexandria Engineering Journal*. (2015).

[Mac+07] Machanavajjhala et al. “L-diversity: Privacy beyond k-anonymity”. In: *ACM Transactions on Knowledge Discovery from Data*. (2007).

[Mah+02] Mahajan et al. “Controlling high bandwidth aggregates in the network”. In: *ACM SIGCOMM Computer Communication Review*. (2002).

[Mar+07] Mariyasagayam et al. “Enhanced multi-hop vehicular broadcast for active safety applications”. In: *7th International Conference on ITS Telecommunications*. (2007).

[Men+18] Meneguette et al. *Intelligent Transport System in Smart Cities*. Springer, 2018. ISBN: 978-3-319-93332-0.

[Met02] Metz. “IP anycast point-to-(any) point communication”. In: *IEEE Internet Computing* (2002).

[Mil+87] Miller et al. *Section E. 2.1: Kerberos authentication and authorization system*. 1987.

[Mis+16] Mishra et al. “VANET security: Issues, challenges and solutions”. In: *International Conference on Electrical, Electronics, and Optimization Techniques*. (2016).

[Moh+10] Mohseni et al. “Comparative review study of reactive and proactive routing protocols in MANETs”. In: *4th IEEE International Conference on Digital Ecosystems and Technologies*. (2010).

[Mon+11] Mondal et al. “A silent tsunami on indian road: A comprehensive analysis of epidemiological aspects of road traffic accidents”. In: *British Journal of Medicine and Medical Research*. (2011).

[MP19] Miller and Pelsser. “A Taxonomy of Attacks using BGP Blackholing”. In: *European Symposium on Research in Computer Security*. (2019).

[MS15] Molinaro and Scopigno. *VANET standards, solutions, and research*. Springer International Publishing Switzerland, 2015. ISBN: 978-3-319-15496-1.

[Nau+09] Naumann et al. “VSimRTI – Simulation runtime infrastructure for V2X communication scenarios”. In: *16th ITS World Congress and Exhibition on Intelligent Transport Systems and Services*. (2009).

[Nau+10] Naumann et al. “Incidence and total lifetime costs of motor vehicle–related fatal and nonfatal injury by road user type, United States, 2005”. In: *Traffic Injury Prevention*. (2010).

[ND04] Nordström and Dovrolis. “Beware of BGP attacks”. In: *ACM SIGCOMM Computer Communication Review*. (2004).

[Ngu+16] Nguyen et al. “An efficient time slot acquisition on the hybrid TDMA/CSMA multi-channel MAC in VANETs”. In: *IEEE Communications Letters*. (2016).

[NO14] Nowdehi and Olovsson. “Experiences from implementing the ETSI ITS SecuredMessage service”. In: *IEEE Intelligent Vehicles Symposium Proceedings*. (2014).

[Now13] Nowdehi. “Vulnerability assessment of secured message and identity management services in ETSI ITS V2V Communications”. MA thesis. Chalmers University of Technology, 2013.

[NS78] Needham and Schroeder. “Using encryption for authentication in large networks of computers”. In: *Communications of the ACM*. (1978).

[NY90] Naor and Yung. “Public-key cryptosystems provably secure against chosen ciphertext attacks”. In: *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*. (1990).

[OF17] Obermaier and Facchi. “Observations on OMNeT++ real-time behaviour”. In: *arXiv preprint arXiv:1709.02207*. (2017).

[Oma+12] Omar et al. “VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs”. In: *IEEE Transactions on Mobile Computing*. (2012).

[Org15] World Health Organization. “Global status report on road safety”. (2015).

[Pat11] Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2011. ISBN: 978-1-4398-1920-3.

[Pau+12] Paul et al. “VANET routing protocols: Pros and cons”. In: *arXiv Preprint arXiv:1204.1201*. (2012).

[PB94] Perkins and Bhagwat. “Highly dynamic destination-sequenced distance-vector routing for mobile computers”. In: *ACM SIGCOMM Computer Communication Review*. (1994).

[PC97] Park and Corson. “A highly adaptive distributed routing algorithm for mobile wireless networks”. In: *Proceedings of INFOCOM*. (1997).

[Pen+07] Peng et al. “Survey of network-based defense mechanisms countering the DoS and DDoS problems”. In: *ACM Computing Surveys* (2007).

[Pet+14] Petit et al. “Pseudonym schemes in VANETs: A survey”. In: *IEEE Communications Surveys & Tutorials* (2014).

[PH15] Ponikwar and Hof. “Overview on security approaches in ITS”. In: *arXiv Preprint arXiv:1509.01552*. (2015).

[PJ08] Papadimitratos and Jovanovic. “GNSS-based positioning: Attacks and countermeasures”. In: *IEEE Military Communications Conference*. (2008).

[PK01] Pfitzmann and Köhntopp. “Anonymity, unobservability, and pseudonymity – A proposal for terminology”. In: *Designing Privacy Enhancing Technologies*. (2001).

[Pos80] Postel. *RFC 768: UDP*. (1980).

[Pos81] Postel. *RFC 761: TCP*. (1981).

[PR99] Perkins and Royer. “Ad hoc on-demand distance vector routing”. In: *Proceedings WMCSA. 2nd IEEE Workshop on Mobile Computing Systems and Applications*. (1999).

[Pur+17] Purohit et al. “Mitigation and performance analysis of routing protocols under black-hole attack in VANETs”. In: *Wireless Personal Communications*. (2017).

[Qu+15] Qu et al. “A security and privacy review of VANETs”. In: *IEEE Transactions on ITS*. (2015).

[Ram+03] Ramaswamy et al. “Prevention of cooperative black hole attack in wireless ad hoc networks.” In: *International Conference on Wireless Networks*. (2003).

[Ras+17] Rasheed et al. “VANETs: A survey, challenges, and applications”. In: *VANETs for Smart Cities*. (2017).

[RD13] Rani and Dhir. “A study of ad-hoc networks: A review”. In: *International Journal of Advanced Research in Computer Science and Software Engineering*. (2013).

[Rez+14] Rezaei et al. “Extent, consequences and economic burden of road traffic crashes in Iran”. In: *Journal of Injury and Violence Research*. (2014).

[RH05] Raya and Hubaux. “The security of VANETs”. In: *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*. 2005.

[RH10] Riley and Henderson. “The NS-3 network simulator”. In: *Modeling and Tools for Network Simulation*. (2010). ISBN: 978-3-642-12331-3.

[Rie+15] Riebl et al. “Artery: Extending Veins for VANET applications”. In: *International Conference on Models and Technologies for ITS*. 2015.

[Rie+17] Riebl et al. “Vanetza: Boosting research on inter-vehicle communication”. In: *Proceedings of the 5th GI/ITG KuVS Fachgespräch Inter-Vehicle Communication*. (2017).

[Rie+19] Riebl et al. “Artery: Large scale simulation environment for ITS applications”. In: *Recent Advances in Network Simulation*. (2019).

[Ros+13] Roscher et al. “ezCar2X: a modular software framework for rapid prototyping of V2X applications”. In: *9th ITS European Congress*. (2013).

[RS91] Rackoff and Simon. “Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack”. In: *Annual International Cryptology Conference*. (1991).

[SA14] Singh and Agrawal. “VANET routing protocols: Issues and challenges”. In: *Recent Advances in Engineering and Computational Sciences*. (2014).

[Sae+12] Saeed et al. “MANET routing protocol taxonomy”. In: *International Conference on Future Communication Networks*. (2012).

[SAR17] Samara and Al-Raba’nah. “Security issues in VANETs: a survey”. In: *arXiv Preprint arXiv:1712.04263*. (2017).

[Sch+06] Schmitz et al. “Analysis of path characteristics and transport protocol design in VANETs”. In: *63rd IEEE Vehicular Technology Conference*. (2006).

[SD02] Serjantov and Danezis. “Towards an information theoretic metric for anonymity”. In: *International Workshop on Privacy Enhancing Technologies*. (2002).

[Shu+16] Shukla et al. “Security in VANETs by using multiple operating channels”. In: *3rd International Conference on Computing for Sustainable Global Development*. (2016).

[Sie+17] Siegel et al. “A survey of the connected vehicle landscape – Architectures, enabling technologies, applications, and development areas”. In: *IEEE Transactions on ITS*. (2017).

[Sin+14] Singh et al. “Cognitive radio for VANETs: Approaches and challenges”. In: *EURASIP Journal on Wireless Communications and Networking*. (2014).

[Sjö+16] Sjöberg et al. “C-ITS deployment in Europe – Current status and outlook”. In: *arXiv Preprint arXiv:1609.03876*. (2016).

[Sma+01] Smalley et al. “Implementing SELinux as a Linux security module”. In: *NAI Labs Report* (2001).

[Sno+01] Snoeren et al. “Hash-based IP traceback”. In: *ACM SIGCOMM Computer Communication Review*. (2001).

[Som+08] Sommer et al. “Simulating the influence of inter-vehicle communication on road traffic using bidirectionally coupled simulators”. In: *IEEE INFOCOM Workshops*. (2008).

[SS17] Sakiz and Sen. “A survey of attacks and detection mechanisms on ITS: VANETs and Internet of Vehicles”. In: *Ad Hoc Networks*. (2017).

[Sta+12] Stallings et al. *Computer security: Principles and practice*. Pearson Education USA, 2012. ISBN: 978-0-13-377392-7.

[Sta+18] Stallings et al. *Computer security: Principles and practice*. Pearson Education USA, 2018. ISBN: 978-0-13-479410-5.

[Sun+00] Sun et al. “GPS-based message broadcasting for inter-vehicle communication”. In: *International Conference on Parallel Processing*. 2000.

[Sun+10] Sun et al. “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communication”. In: *IEEE Transactions on Vehicular Technology*. (2010).

[TD17] Tyagi and Dembla. “Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of VANETs”. In: *Egyptian Informatics Journal*. (2017).

[TK84] Takagi and Kleinrock. “Optimal transmission ranges for randomly distributed packet radio terminals”. In: *IEEE Transactions on Communications*. (1984).

[Tom+14] Tomandl et al. “VANETsim: An open source simulator for security and privacy concepts in VANETs”. In: *International Conference on High Performance Computing Simulation*. (2014).

[TS07] Tamilselvan and Sankaranarayanan. “Prevention of black hole attacks in MANETs”. In: *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*. (2007).

[TS08] Tamilselvan and Sankaranarayanan. “Prevention of cooperative black hole attacks in MANET.” In: *Journal of Networks*. (2008).

[Tse+18] Tseng et al. “Black hole along with other attacks in MANETs: A survey”. In: *Journal of Information Processing Systems*. (2018).

[UR10] Ullah and Rehman. “Analysis of black hole attacks on MANETs using different MANET routing protocols”. MA thesis. Blekinge Institute of Technology, 2010.

[Var10] Varga. “OMNeT++”. In: *Modeling and Tools for Network Simulation*. Springer Berlin Heidelberg, 2010. ISBN: 978-3-642-12330-6.

[Ver+13] Verma et al. “An efficient defense method against UDP spoofed flooding traffic of DoS attacks in VANET”. In: *3rd IEEE International Advance Computing Conference*. (2013).

[Ver17] Vermeulen. *SELinux System Administration*. Packt Publishing Limited, 2017. ISBN: 978-1-78712-695-4.

[Wai89] Waidner. "Unconditional sender and recipient untraceability in spite of active attacks". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. (1989).

[Wex+08] Wex et al. "Trust issues for VANETs". In: *IEEE Vehicular Technology Conference*. (2008).

[WK05] Wang and Kar. "Throughput modelling and fairness issues in CSMA/CA-based ad hoc networks". In: *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies*. (2005).

[Woo+15] Woo et al. "A practical wireless attack on the connected car and security protocol for in-vehicle CAN". In: *IEEE Transactions on ITS*. (2015).

[Yad+11] Yadav et al. "Security in VANETs". In: *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC Press, 2011. ISBN: 978-1-4398-1920-3.

[Yan+04] Yang et al. "Security in MANETs: Challenges and solutions". In: *IEEE Wireless Communications*. (2004).

Online References

[Boj+a] Bojthe et al. *INET*. Access: 2020-07-09. URL: `https://github.com/inet-framework/inet`.

[Boj+b] Bojthe et al. *INET forked by Riebl*. Access: 2020-07-09. URL: `https://github.com/riebl/inet/`.

[Cen] German Aerospace Center. *Website of SUMO*. Access: 2020-07-09. URL: `https://sumo.dlr.de/docs/index.html`.

[Cod+] Codecá et al. *LuST scenario*. Access: 2020-07-09. URL: `https://github.com/lcodeca/LuSTScenario`.

[Con05] FlexRay Consortium. *FlexRay communications system protocol specification version 2.1*. Access: 2020-07-09. (2005). URL: `https://www.softwareresearch.net/fileadmin/src/docs/teaching/SS08/PS_VS/FlexRayCommunicationSystem.pdf`.

[Con10] LIN Consortium. *LIN: specification package revision 2.2 A*. Access: 2020-07-09. (2010). URL: https://www.cs-group.de/wp-content/uploads/2016/11/LIN_Specification_Package_2.2A.pdf.

[Cur15] Currie. *Developments in car hacking*. Access: 2020-07-09. (2015). URL: https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607.

[Env16] Ricardo Energy & Environment. *Study on the deployment of C-ITS in Europe: Final report*. Access: 2020-07-09. (2016). URL: https://ec.europa.eu/transport/sites/transport/files/2016-c-its-deployment-study-final-report.pdf.

[Gmb91] Robert Bosch GmbH. *Specification, CAN*. Access: 2020-07-09. (1991). URL: http://esd.cs.ucr.edu/webres/can20.pdf.

[Inc] Amazon.com Inc. *Amazon website*. Access: 2020-07-09. URL: https://www.amazon.de/.

[Inga] Technische Hochschule Ingolstadt. *Github repository of Artery*. Access: 2020-07-09. URL: https://github.com/riebl/artery.

[Ingb] Technische Hochschule Ingolstadt. *Github repository of Vanetza*. Access: 2020-07-09. URL: https://github.com/riebl/vanetza.

[Ins] European Telecommunications Standards Institute. *ETSI website*. Access: 2020-07-09. URL: https://www.etsi.org.

[Jak+] Jakob et al. *Pybind11*. Access: 2020-07-09. URL: https://github.com/pybind/pybind11/.

[Kis13] Kissel. *Glossary of key information security terms, NISTIR 7298 revision 2*. Access: 2020-07-09. (2013). URL: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[Mmi] *MMITSS Final ConOps*. Access: 2020-07-09. University of Arizona et al., 2014. URL: http://www.cts.virginia.edu/wp-content/uploads/2014/05/Task2.3._CONOPS_6_Final_Revised.pdf.

[MV13] Miller and Valasek. *Adventures in automotive networks and control units*. Access: 2020-07-09. (2013). URL: http://illmatics.com/car_hacking.pdf.

[MV14] Miller and Valasek. *A survey of remote automotive attack surfaces*. Access: 2020-07-09. (2014). URL: http://illmatics.com/remote%20attack%20surfaces.pdf.

[MV15] Miller and Valasek. *Remote exploitation of an unaltered passenger vehicle*. Access: 2020-07-09. (2015). URL: http://illmatics.com/Remote%20Car%20Hacking.pdf.

[Nie+17] Nie et al. *Free-fall: Hacking tesla from wireless to CAN bus*. Access: 2020-07-09. (2017). URL: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf.

[PC] iTetris Project Consortium. *Website of iTetris*. Access: 2020-07-09. URL: http://www.ict-itetris.eu/.

[PH10] Pfitzmann and Hansen. *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. Access: 2020-07-09. (2010). URL: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[Som+] Sommer et al. *Veins*. Access: 2020-07-09. URL: https://github.com/sommer/veins.

[Sto+04] Stoneburner et al. *NIST special publication 800-27 revision A*. Access: 2020-07-09. (2004). URL: https://csrc.nist.gov/publications/detail/sp/800-27/rev-a/archive/2004-06-21.

[Vir+] Virdis et al. *SimuLTE forked by Riebl*. Access: 2020-07-09. URL: https://github.com/riebl/simulte/.

[Vor+a] Voronov et al. *Geonetworking: Vehicle adapter*. Access: 2020-07-09. URL: https://zenodo.org/record/51295.

[Vor+b] Voronov et al. *Implementation of ETSI ITS-G5 GeoNetworking stack, in Java: CAM-DENM/ASN.1 PER/BTP/GeoNetworking*. Access: 2020-07-09. URL: https://zenodo.org/record/55650.