Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review

Abasi-Amefon O. Affia(✉), Raimundas Matulevičius, and Alexander Nolte

Institute of Computer Science, University of Tartu, Tartu, Estonia
{amefon.affia,rma,alexander.nolte}@ut.ee

Abstract. The automotive industry is maximizing cooperative interactions between vehicular sensors and infrastructure components to make intelligent decisions in its application (i.e., traffic management, navigation, or autonomous driving services). This cooperative behaviour also extends to security. More connected and cooperative components of vehicular intelligent transportation systems (ITS) result in an increased potential for malicious attacks that can negatively impact security and safety. The security risks in one architecture layer affect other layers of ITS; thus, cooperation is essential for secure operations of these systems. This paper presents results from a comprehensive literature review on the state-of-the-art of security risk management in vehicular ITS, evaluating its assets, threats/risks, and countermeasures. We examine these security elements along the dimensions of the perception, network, and application architecture layers of ITS. The study reveals gaps in ITS security risk management research within these architecture layers and provides suggestions for future research.

Keywords: Cooperative intelligent transportation systems (ITS) · vehicular ITS · Internet of Things (IoT) · STRIDE · Information System Security Risk Management (ISSRM)

1 Introduction

Transportation is one of the cornerstones of human civilization, facilitating the mobility of people and goods. Intelligent transportation systems (ITS) provide such mobility through cooperative sensing, processing, and communication technologies [13]. To improve transportation efficiency in an ITS, sensors and objects have to interact to collect and exchange data over vehicular and infrastructure networks, and make intelligent predictions and decisions.

Due to the potential threat to critical business assets and the possible catastrophic physical effects that can endanger human lives [18,20] it is essential to consider ITS security covering all its components [20]. Security threats in this domain are multifaceted, including transportation, IoT, and distributed system type threats to ITS components and thus require security risk management.

H. Panetto et al. (Eds.): OTM 2019, LNCS 11877, pp. 282–300, 2019.
https://doi.org/10.1007/978-3-030-33246-4_18

ITS security risk management [28,41,42] is crucial to ensure the confidentiality, integrity, and availability of the data that is being collected and aggregated to ensure safe and efficient operation of transportation systems (e.g., speed management, navigation and traffic management [13]). There is thus a need to understand the current state of ITS security risk research related to the cooperative architecture of ITS. We seek to provide an overview of the current start-of-the-art in this field to foster continuous research and development of ITS security risk management by addressing the following main research question:

How can we manage security risks in ITS?

To answer this research question, we conducted a systematic literature review (SLR) (following the [26] guidelines) to aggregate existing analysis on security risk management in vehicular ITS [56]. We then analyze the results following the security risk management ontology [14].

The contribution of this paper is threefold. First, based on [30,51,52,54], we provide an overview of the ITS architecture and its protected assets. Second, we provide a state-of-the-art overview of security threats and their countermeasures within each ITS architecture layer. Third, we discuss the current state of security management research in ITS and highlight future research directions.

2 Background

In this section we ground our work in existing literature covering ITS, its structure, security risk management in information systems and secondary studies on IoT security risk management (Sect. 2.3).

2.1 Overview of ITS

ITS – based on the internet-of-things (IoT) paradigm [5] – utilize cooperative sensing and networking capabilities to manage people and goods for transportation via road, air, rail, and water. ITS encompass systems responsible for the collection, storage, transmission and manipulation of data involving vehicles, individuals (drivers, passengers, road operators, and managers), mobile devices and infrastructure (road units, video monitoring, traffic lights, internet) cooperating within each other and the environment [41]. System components include (*i*) systems that collect data (*ii*) systems that transmit collected data and (*iii*) systems that provide the data to end-users following predefined processes [41].

ITS can be perceived as IoT system since they consist of various objects that form a cooperative system to reach a common goal [2]. IoT systems consist of three architectural layers [30,51–55] as illustrated in Fig. 1:

- Perception: The perception layer consists of hardware and software components (sensors, actuators, visioning, and positioning devices), carrying out basic functions such as collecting, controlling, and storing data.

– Network: The network layer facilitates wireless or wired transmission (in-vehicle, vehicle to vehicle, and vehicle to infrastructure) of collected data from perception components.
– Application: The application layer connects the network layer with the end-user, application processes, computing, and storage, allowing high-level intelligent processing of the generated and transmitted data. These applications include speed and traffic management [17,23,43,48], navigation [6,36], and driver-related services [4,7,32,46,49] in the context of ITS.

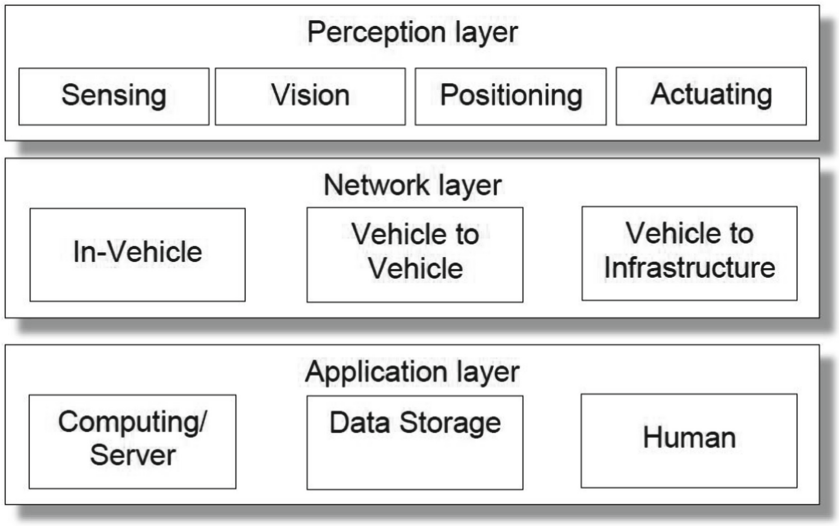

Fig. 1. Architecture layers of ITS

The layers are interconnected having a high impact on connected layers and collectively serving to deliver better mobility improvements for various forms of transport [13]. Dependencies between layers demand thorough security risk management consideration within all three layers to ensure confidentiality, integrity, and availability of data.

2.2 Security Risk Management

"*Security engineering* is concerned with lowering the risk of intentional unauthorized harm to valuable assets to a level acceptable to the system's stakeholders by preventing and reacting to malicious threats and security risks" [18]. Hence, security in the context of this paper deals specifically with intentional unauthorized threats and risks that explicitly pose harm to system assets. Security engineering is thus different from safety engineering dealing with unintentional risk, and privacy engineering dealing with accidental information leakage.

Previous work on security risk management methods [14] covers a number of standards and methods [9,16,25] to secure assets and manage security or security

risks. The review conducted by Dubois et al. [14] resulted in the development of the ISSRM method and its domain model, compliant to the concepts and definitions we found in our review of security standards and methods. The ISSRM domain model (see Fig. 2) consists of an ontology to compare, select, or improve security risk management methods used in organizations. This domain model suggests three conceptual parts covering *assets* (business and system assets), *security risks* and *countermeasures*.

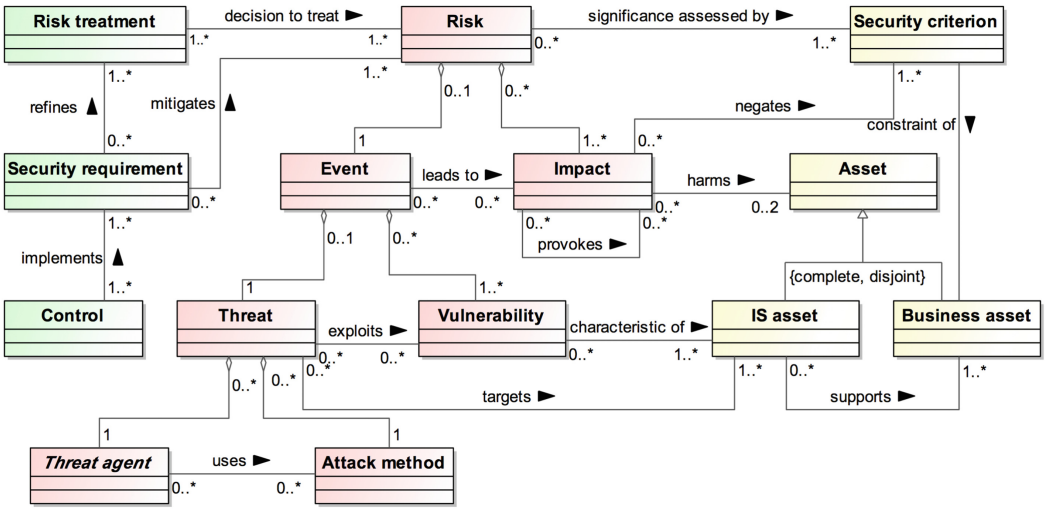

Fig. 2. ISSRM domain model adapted from [14,33]

- *Asset-related concepts*: *Business assets* are defined as information, data and processes that bring value to an organization. *System/IS assets* support *business assets*. *Security criteria* (confidentiality, integrity and availability) are constraints that define the security needs [14] of each *business asset*.
- *Security risk-related concepts*: A *security risk* is the combination of a security *event* and its *impact* (negation of the security criterion harming at-least a business and IS asset, c.f. Sect. 5.1 for an example scenario). A risk *event* is defined as the aggregation of a *threat* that exploits a *vulnerability* [33]. A *vulnerability* is a characteristic of a system asset, constituting its weakness. A *threat* targets a system asset by exploiting its vulnerability. It is a combination of a *threat agent* – an entity with interests to harm the assets – and an *attack method* – the means to carry out the threat. Methods of discovering this *threat* combination have been proposed and developed by security experts [24]. We selected the STRIDE method [44] for security threat analysis for this work due to its industrial usage, maturity, and high research concentration within the security community.
  The abbreviation STRIDE stands for *Spoofing (S)* – pretending to be something or someone, *Tampering (T)* – modifying something that you are not supposed to modify, *Repudiation (R)* – claiming you didn't do something (regardless of if this is true or not), *Information Disclosure (I)* – exposing

information to those who are not authorized to view it, *Denial of Service (D)* – attacks designed to prevent a system from providing its intended service by crashing it, slowing it down, or filling ts storage, and *Elevation of Privilege (E)* – when a program or user can to do things (technically) that they are not supposed to be able to do [44]. We use STRIDE to elicit and categorize security threats as well as for risk treatment.

– *Security risk treatment* concepts include *security requirements* that define conditions to be reached by mitigating the security risks and the *controls* implement the defined security requirements. Security requirements can be classified into different types [19] including identification, authentication, authorization, immunity, integrity, intrusion detection, non-repudiation. Each type of security requirement potentially corresponds and mitigates threats covered by STRIDE [44]: Spoofing can be mitigated by *Authentication*, Tampering - *Integrity*, Repudiation - *Non-repudiation*, Information Disclosure - *Confidentiality*, Denial of Service - *Availability* and Elevation of privilege - *Authorization*.

2.3 Secondary Studies

Secondary studies have been carried out in literature [53,55] to analyze assets, threats, and security solutions in IoT security architecture. This paper, however, presents a study of these cooperative architecture layers, focusing on ITS asset, risk, and risk treatment concepts. We assess ITS security risk management efforts following the ISSRM domain model [14].

3 Review Protocol

Figure 3 illustrates the review protocol used for this work. It is based on the proposed guidelines by Kitchenham *et al.* [26]. The review goal is to survey primary literature covering security risks in ITS.

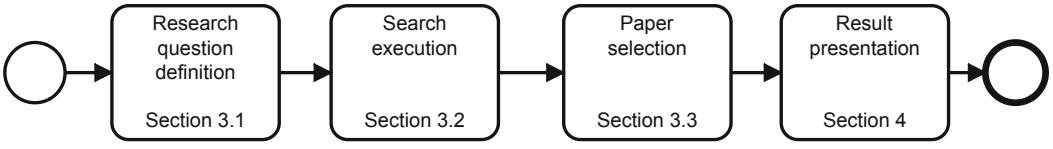

Fig. 3. Systematic literature review protocol

3.1 Research Question Definition

We derived the following the sub-questions from our main research question to study security risk management in ITS:

RQ$_1$. *How are asset-related concepts in ITS addressed?*

RQ$_2$. *How are risk-related concepts in ITS addressed?*
RQ$_3$. *How are risk treatment-related concepts in ITS addressed?*

RQ$_1$ focuses on assets that are of high value to vehicular ITS. We thus focus on assets that will have a considerable impact in the event of a security threat and therefore pose a security risk. **RQ**$_2$ focuses on known threats to ITS and their resulting risks. **RQ**$_3$ focuses on countermeasures for risks to each ITS layer. We use the research questions to generate keywords used in the search process for relevant studies within the ITS domain (see Sect. 3.2).

3.2 Search Process

For our review, we used selected digital libraries, including IEEE Explorer, Science Direct, ACM Digital Library, and Springer. The search queries include *"Transport system, intelligent transportation systems, vehicles, smart car, connected vehicles, security threats, security vulnerabilities, security countermeasure"*. These search queries are connected using Boolean operators tailored to each digital library. Also, we conducted manual searches [3,50] to complement the search procedure. Table 2 shows the results of the search results from the sources. We identified a total of 134 results (see Table 2) from which we eventually selected 26 for analysis based on the following inclusion/exclusion criteria.

3.3 Paper Selection

We subjected the identified papers to an initial screening which covered title, keywords, abstract, results, and conclusion. To select relevant papers, we applied the following two filters based on our research questions:

1. **Filter 1:** Applying inclusion/exclusion criteria in Table 1 on the selected papers. Table 2 presents the results of applying the inclusion/exclusion criteria resulting in a total of 58 results.
2. **Filter 2:** Quality assessment of the papers that passed Filter 1 following the Kitchenham quality guidelines [27], with the questions:
   - Does the study cover the scope of work?
   - Does the study describe security risks on information transportation systems?
   - Does the study provide the countermeasures to mitigate security risks?

   The answers to above questions are scored as follows: 1 = Fully satisfied, 0.5 = Partially satisfied, 0 = Not satisfied. We included studies with 2.5 or more points, resulting in a total of 26 final paper for data extraction and further analysis (see Table 2).

Table 1. Inclusion/exclusion criteria on the selected papers

Inclusion criteria	Exclusion criteria
Papers in the area of IoT, research scope is cooperative ITS and sub-scope of vehicular ITS	Papers that focus on security in limited aspects of vehicular transportation systems
Papers that explicitly carry out security risk assessment or analysis	Papers that discuss safety – unintentional harm to systems
Papers that present security risk solutions	Non-English papers
Academic papers that are accessible in full text from the university	Duplicate works

Table 2. Selected sources and corresponding results for literature review

Sources	IEEE	ACM	Springer	ScienceDirect	Manual	Total
Returned	18	43	49	14	10	134
Filter 1	14	12	15	8	9	58
Filter 2 (Final selection)	6	7	4	2	7	26

3.4 Threats to Validity

There are multiple threats to the validity of this work. First, the derived keywords might not adequately address the scope defined by the research questions. Second, we might have missed relevant articles due to the quality of the keywords. Third, the studies selected might not meet scientific standards. To mitigate these threats, we conducted quality assessments based on the inclusion/exclusion criteria. Finally, the adoption of a three layers ITS model may pose a threat. Nonetheless, this work follows the IoT structure/layer state-of-art that propose these three layers as well.

4 Result Presentation

In this section, we summarize the results of our analysis. From 134 articles investigated, we discarded 108 papers while applying the filters from Sect. 3.3. The remaining 26 papers were analyzed to answer the research questions.

4.1 Protected Assets

Table 3 summarises ITS assets (system and business assets), classify these assets and in addition, illustrate basic functional areas of each layer.

Table 3. Architecture layer assets

Layer	System assets		Business assets
Perception [10]	Sensing	Light detection and ranging (LiDAR), visible light communication (VLC), ultrasonic ranging devices (URD), millimeter wave radar, thermometer and infrared ranging	Ultrasonic data, radio frequencies, heat measurement, traffic count, travel time, vehicle weight data
	Vision	Video cameras, HD cameras, stereo vision systems, and Closed-circuit television camera (CCTV)	Surveillance (picture and video) data, 3D imaging data, traffic count
	Positioning	Global positioning system (GPS) receiver and radars (doppler radar speedometers, radar cruise control, and radar based obstacle detection systems)	Pseudo-range measurements, travel speed, radar data, vehicle location data
	Actuating	Vehicle node, ECU, key/remote device, infotainment	Mileage measurement, error codes, event data records, traffic warning messages, key/remote signal, transaction information
Network [31]	In-vehicle network	Controller area network (CAN), automotive Ethernet, byteflight, FlexRay, local interconnect network (LIN), low-voltage differential signaling (LVDS), and media oriented systems transport (MOST)	Perception data (e.g., tire pressure monitoring system (TPMS) messages)
	Vehicle-to-vehicle (V2V) network	Dedicated short range communications (DSRC)/wireless access in vehicular environments (WAVE), LTE/5G, worldwide interoperability for microwave access (WiMAX)	Perception data (e.g., travel direction, vehicle range data)
	Vehicle-to-infrastructure (V2I) network		Perception data (e.g., Traffic count, accident data, transaction information, vehicle range data)
Application [12]	Computing/Server	Web application server (parking space allocation server, central parking server)	Application service, application process, application data, perception data (e.g., key/remote signal, vehicle location data)
	Data Storage	Data center, Edge data center (Fog)	Perception data (e.g., vehicle location data)
	Human	User, Driver, Administrator	Application process

Perception Layer Assets are illustrated in Table 3. This layer consists of devices for sensing (e.g., ranging devices, thermometers), vision (e.g., Closed-circuit television camera (CCTV), HD camera), positioning (e.g., GPS receiver and Radars) and actuating (e.g., ECU, key/remote device). These devices are system assets that support data perception and primary actuating functions. The business assets are data generated or stored at this layer supported by its system assets. For example heat measurement (sensing – thermometers), surveillance data (vision – CCTV, HD camera), pseudo-range measurements (positioning – GPS receiver), and error codes (actuating – engine control unit (ECU)).

Network Layer Assets cover in-vehicle networks facilitating the transmission of data collected from the perception layer (e.g., controller area network (CAN), vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)). Related business assets include, e.g., tire pressure monitoring systems (TPMS) messages (supported by CAN) and vehicle range data (supported by V2V or V2I).

Application Layer Assets collated in Table 3 cover computing/server devices (e.g., web application server), data storage devices (e.g., data center), and human assets (e.g., driver, administrator). Examples for business assets are smart application services (running on a web application server), vehicle location data (stored in a data storage) and application processes (executed by the driver).

4.2 Security Risks

We have defined security risk-related concepts in Sect. 2.2 which covers *vulnerability*, *threat*, *impact*, and the resulting *risk*. While not all risk-related concepts are fully covered in ITS security research, *threat* risk-related concept is widely covered. Tables 4, 5, and 6 summarize security threats at different architectural layers of ITS. We categorized these threats following the STRIDE threat model.

Perception Layer Threats (see Table 4) include threats to sensing, vision, positioning and actuating ITS components. The spoofing category (S) contains 6 threats (15 occurrences) with spoofing reported to be the most common. The tampering (T) presents 5 threats (6 occurrences) with tampering reported to be the most common. The repudiation (R) presents 1 threat – bogus messages. The information disclosure (I) contains 2 threats – stored attacks and eavesdropping each having 1 occurrence. The denial of service (D) presents 5 threats (6 occurrences) with jamming reported to be the most common. Lastly, the elevation of privilege (E) contains 5 threats (6 occurrences) with malware to be the most common.

Network Layer Threats are covered in Table 5. These threats affect the ability of system assets to transmit necessary data for ITS functions. ITS typically transmits data through in-vehicle, vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) communication technologies. The spoofing category (S)

Table 4. Perception layer security threats

System Asset	Security Threats					
	S	T	R	I	D	E
Sensing, Positioning, and Vision Technologies	Spoofing (6), Node Impersonation (1), Illusion (3), Replay (3), Sending deceptive messages (1), Masquerading (1)	Forgery (1), Data manipulation (1), Tampering (2), Falsification of readings (1), Message Injection (1)	Bogus message (1)	Stored attacks (1), Eavesdropping (1)	Message saturation (1), Jamming (3), DoS (1), Disruption of system (1)	Backdoor (1), Unauthorised access (1), Malware (2), Elevation of privilege (1) Remote update of ECU (1)
Total	6 threats (15 occurrences)	5 threats (6 occurrences)	1 threat (1 occurrence)	2 threats (2 occurrences)	5 threats (6 occurrences)	5 threats (6 occurrences)

contains 12 threats (56 total occurrences) with spoofing threat reported to be the most common (13 occurrences). The tampering category (T) contains 7 threats (29 total occurrences) with injection (message, command, code, packet) and manipulation/alteration/fabrication/modification reported to be the most common (7 occurrences each). The repudiation category (R) contains 3 threats (5 total occurrences) with bogus messages reported to be the most common (3 occurrences). The information disclosure category (I) contains 11 threats (30 total occurrences) with eavesdropping reported to be the most common (10 occurrences). The denial of service category (D) contains 7 threats (29 total occurrences) with denial of service/distributed denial of service (DoS/DDoS) reported to be the most common (10 occurrences). Lastly, the elevation of privilege category (E) contains 7 threats (16 total occurrences) with malware reported to be the most common (7 occurrences).

Application Layer Threats (see Table 6) involve attacks to disrupt or corrupt high level ITS processes and services enabling intelligent transportation. In the application layer, the spoofing category (S) contains 3 threats (3 total occurrences) with spoofing, sybil and illusion attack, each having 1 occurrence in literature. The tampering category (T) contains 1 threat – malicious update (1 total occurrence) in literature. The repudiation category (R) contains no threats in literature for this layer. The information disclosure category (I) contains 3 threats (4 total occurrences) with eavesdropping reported to be the most common (2 occurrences). The denial of service category (D) contains 1 threat – DoS (2 total occurrences). Lastly, the elevation of privilege category (E) contains 4 threats (4 total occurrences) with malware, jail-breaking OS, social engineering and rogue data-center each reported to be the most common (1 occurrence each) in literature.

Table 5. Network layer security threats

System asset	Security threats					
	S	T	R	I	D	E
In-vehicle network, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure technologies (V2I)	Sybil (10), Spoofing (GPS) (13), Replay attack (11), Masquerading (7), RF Fingerprinting (1), Wormhole (6), Camouflage attack (1), Impersonation attack (2), Illusion attack (2), Key/Certificate Replication (1), Tunneling (1), Position Faking (1)	Timing attacks (1), Injection (message, command, code, packet) (7), Manipulation/Alteration/Fabrication/Modification (7), Routing modification/manipulation (5), Tampering(broadcast, message transaction, hardware) (6), Forgery (1), Malicious update (software/firmware) (2)	Bogus messages (3), Rogue Repudiation (1), Loss of event trace-ability (1)	Eavesdropping (10), Man-in-the-middle (5), ID disclosure (1), Location tracking (5), Data sniffing (1), Message interception (2), Information disclosure (1), Traffic analysis (1), Information gathering (1), TPMS tracking (1), Secrecy attacks (1)	DoS/DDoS (10), Spam (5), Jamming (5), Flooding (3), Message suppression (1), Channel interference (1), Black hole (4).	Malware (7), Brute Force (2), Gaining control (1), Social engineering (3), Logical attacks (1), Unauthorised access (1), Session Hijack (1)
Total	12 threats (56 occurrences)	7 threats (29 occurrences)	3 threats (5 occurrences)	11 threats (30 occurrences)	7 threats (29 occurrences)	7 threats (16 occurrences)

Table 6. Application layer security threats

System asset	Security threats					
	S	T	R	I	D	E
Application server, Edge data center, Human	Spoofing (1), Sybil (1), Illusion attack (1)	Malicious Update (1)		Eavesdropping (2), Location tracking (1), Privacy leakage (1)	DoS (2)	Jail-breaking OS (1), Social engineering (1), Rogue Data-center (1), Malware (1)
Total	3 threats (3 occurrences)	1 threat (1 occurrence)	0	3 threats (4 occurrences)	1 threat (2 occurrence)	4 threats (4 occurrences)

4.3 Security Countermeasures

We illustrate the security countermeasures proposed in surveyed literature to address security risks in ITS for each layer in Table 7. Security risks are classified into the following security requirements: confidentiality, integrity, availability, authentication, authorization, and non-repudiation. Our findings indicate that related work mainly covers network layer threats, e.g., spoofing by authentication controls and denial of service by availability controls. Repudiation category threats in the network and application layers and denial of service category threats in the perception and application layers are not as frequently covered. However, we did not identify non-repudiation and availability countermeasures to mitigate security threats.

Table 7. Security countermeasures in ITS layers.

Security Req types	Perception layer	Network layer	Application Layer
Authentication	Spoofing resistant positioning system [38], device level user authentication [40], digital certificates, digital signature of software and sensors [10,34], challenge/response mechanism [34], encrypted Precise Positioning System (PPS)	ID authentication [15], radio-frequency identification (RFID) tokens, public key infrastructure [8,47], WAVE security standard [29], secure routing protocol [45], reputation scoring [22], central validation authority (CVA) [21,34], secure location verification [34], digital certificates and digital signatures [10,22,34], bit commitment and zero-knowledge mechanisms [34], variable MAC and IP addresses, challenge/response mechanism [34]	Digital certificates and digital signatures [10,34]
Integrity	Restricted physical access [10], challenge/response mechanism [34], use trusted hardware piratically impossible to alter existing values unless authorised [34]	Public key infrastructure (PKI) [1,15], hashing function, cryptographic primitives [34], security protocol [15], plausibility validation network (PVN) [1]	Plausibility Validation [35]
Non-repudiation	Use trusted hardware piratically impossible to alter existing values unless authorised [34]		
Confidentiality	Encryption [47]	Vision integrated pseudorange error removal (VIPER) algorithm [34], encryption [15,34,47], secure routing protocol [45], key management [11,15,45], digital signatures [11,15], WAVE security standard [29], firewall [47]	Firewall [47], cryptography services [29]
Availability		Frequency hopping spread spectrum (FHSS) technique [21,22,34], secure routing protocol [22,45], time stamping mechanism [34], bit commitment and signature based authentication mechanisms [34], WAVE security standard [29], firewall [47]	
Authorization	Threat modelling [45], hardware and software access control [34], upgrading on-board diagnostics (OBD)-II port [11]	Variable MAC and IP addresses [34], WAVE security standard [29], intrusion detection system, honeypot system [11,45]	Firewall [47]

5 Discussion

This study presents results from a literature analysis on security risk management in ITS. From this study, we gained the following three distinct insights:

- the importance of defining security risk-related concepts in the ITS domain.
- research concentration in security risk management within layers of ITS.
- an evaluation of the ITS layer with the lowest research concentration.

This section will present a discussion of these concerns based on our results.

5.1 Security Risk-Related Concepts

The benefits of the ISSRM method, its domain model and domain model concepts for security risk management is highlighted in [14]. However, risk-related concept analysis, in combination with associated asset-related concepts to allow sufficient risk treatment analysis, is lacking in most papers. It is essential to understand the cause of risk, and its consequences on assets to deciding for appropriate countermeasures.

We provide security risk analysis in each ITS layer (Table 8) following the asset-related and risk-related concepts of the domain model. Common threats discovered in each layer were selected to form each scenario. As we consider security risk management concepts in the following examples, concepts relating to the measurement of risk is out of the scope of this work.

- *Perception layer risk example.* Spoofing threat is commonly mentioned in the reviewed literature for the perception layer. In Table 8-column 1, an attacker provides a vehicle GPS receiver with false information about its pseudo-range measurements. When such information is accepted by the vehicle GPS receiver and transmitted to the application layer, it misleads the application, sending wrong location information e.g., in case of an emergency.
- *Network layer risk example.* A common threat in this layer is the Sybil attack. In Table 8-column 2, an attacker can create multiple false identifications. One vehicle can send traffic data associated with multiple identities at the same time, creating the illusion that the same messages come from multiple vehicles. This threat leads to the loss of integrity of traffic data, and an attacker can deceive the traffic management application and other vehicles that there is e.g. a traffic jam.
- *Application layer risk example.* A common threat is the DoS attack. An application layer example is a driver-less valet application [12] where a human driver, having arrived at a parking garage, initiates a parking space allocation service. The vehicle communicates with the parking allocation server to autonomously navigate to the parking space allocated. In Table 8-column 3, an attacker can induce a traffic jam to freeze the driver-less valet application by launching a denial of service attack on the parking space allocation server which for example, does not protect against malicious connections. This attack can lead to a shutdown of the parking space allocation service.

Table 8. Security risk analysis examples in ITS layers

Risk Scenario	Perception Layer *Spoofing* [37]	Network Layer *Sybil Attack* [11]	Application Layer *Denial of Service* [12]
Business Asset	Pseudo-range measurements, location data	Traffic data	Parking space allocation service
Security Criteria	Integrity of Pseudo-range measurements, location data	Integrity of traffic data,	Availability of Parking space allocation service
System Asset	Vehicle GPS receiver	Communication medium V2I (Cloud)	Parking space allocation server
Vulnerability	Vehicle GPS receiver is not spoof resistant	Ease of generation of node identities	Parking space allocation server does not protect against malicious connections
Threat	An attacker carries out a spoofing attack to mislead a vulnerable vehicle GPS receiver and inject counterfeit pseudo-range measurements, disrupting the emergency response system of the vehicle	An attacker creates numerous false identities to create the illusion that the traffic data broadcasts come from multiple vehicles to deceive other vehicles that there is a traffic jam	An attacker induces a traffic jam or to freeze the driver-less valet service by launching a denial of service attack on the parking space allocation server
Impact	loss of integrity of Pseudo-range measurements, location data, the vehicle sends wrong location information in emergency	loss of integrity of traffic data	loss of availability of parking space allocation service
Risk	An attacker carries out a spoofing attack to mislead a vulnerable GPS receiver and inject counterfeit pseudo-range measurements leading to wrong location data transmitted and used by emergency response system	An attacker creates numerous false identities to create the illusion that the traffic data broadcast come from multiple vehicles to deceive other vehicles that there is a traffic jam leading to the loss of integrity of traffic data	An attacker induces a traffic jam to freeze the driver-less valet application by launching a denial of service attack on the parking space allocation server leading to the loss of availability of parking space allocation service

5.2 Security Risk Research Concentration

Research in ITS currently concentrates on vehicular network layers and perception layer devices. Security efforts thus tend to be focused on those layers. Only a few papers discuss security issues of the ITS application layer leading to an incomplete state-of-the-art about security risks in ITS in literature.

The application layer provides functions that connect ITS and end-users. However, this layer is also prone to security risks as it is primarily supported by system assets (web, internet, and cloud services) known for security vulnerabilities [39]. It is thus imperative to encourage risk analysis and to propose countermeasures for this layer. This section evaluates ITS application layer security risk and countermeasure dependencies requiring cooperative security efforts.

Security Risk Impact. Security risk impact in the application layer can stem from attacks within this layer or the perception and network layers forming a ripple effect [35]. A false GPS time originating in the perception layer can e.g., inhibit application processes. Sybil and illusion attacks can flood the application with incorrect information, hindering its service process.

Security Defence. ITS demands cooperative security defence. The application layer can provide defence for threats originating within its layer and perception or network layers. Attacks can be challenging to resolve on the perception and network layer, requiring a significant amount of time and resources to identify and revoke an attacker from negatively impacting ITS. Here, countermeasures can be implemented in the application layer as a last line of defence. To protect against spoofing threats (e.g., sybil, replay, and illusion threats), plausibility checks on information from vehicle nodes to validate the correctness of the data. The application layer can deal with ripple effect risks from other layers. It is also the last line of defence against threats to ITS. Future research within this layer is encouraged to realize its opportunities fully.

6 Concluding Remarks

The possibilities of making intelligent decisions and predictions through functional and operational cooperation within ITS components have created opportunities in the transportation industry, research, and development. This cooperative behaviour extends to security within its functions and operations. In this paper, we presented an extensive and comprehensive literature review on the current state of the art in ITS security risk management along with the layered architecture of IoT – perception, networking, and application layers. ITS stakeholders must ensure the required security criteria (i.e., confidentiality, integrity, and availability) within each architecture layer and its cooperative interactions. We explored in each architecture layer, asset-related concepts to elicit assets, risk-related concepts to document possible threats to these assets, and risk treatment-related concepts to provide security solutions. Also, our research revealed a lack of analysis for risk-related concepts with its connected asset-related concepts to

allow risk treatment-related analysis. Results also reveal low research concentration for the application architecture layer despite its cooperative functional and security importance within ITS layers. Research in the field of ITS security risk management, especially the application layer needs to be explored further to develop innovative security solutions and applications.

Acknowledgments. This paper is supported in part by European Union's Horizon 2020 research and innovation programme under grant agreement No 830892, project SPARTA.

References

1. Al-Kahtani, M.S.: Survey on security attacks in vehicular ad hoc networks (VANETs). In: 2012 6th International Conference on Signal Processing and Communication Systems, pp. 1–9. IEEE (2012)
2. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
3. Badampudi, D., Wohlin, C., Petersen, K.: Experiences from using snowballing and database searches in systematic literature studies. In: Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering, p. 17. ACM (2015)
4. Barth, M., Boriboonsomsin, K.: Energy and emissions impacts of a freeway-based dynamic eco-driving system. Transp. Res. Part D: Transp. Environ. **14**(6), 400–410 (2009)
5. Bojan, T.M., Kumar, U.R., Bojan, V.M.: An Internet of Things based intelligent transportation system. In: 2014 IEEE International Conference on Vehicular Electronics and Safety, pp. 174–179. IEEE (2014)
6. Boriboonsomsin, K., Barth, M.J., Zhu, W., Vu, A.: Eco-routing navigation system based on multisource historical and real-time traffic information. IEEE Trans. Intell. Transp. Syst. **13**(4), 1694–1704 (2012)
7. Cervero, R., Tsai, Y.: City Carshare in San Francisco, California: second-year travel demand and car ownership impacts. Transp. Res. Rec.: J. Transp. Res. Board **1887**(1), 117–127 (2004)
8. Chen, Q., Sowan, A.K., Xu, S.: A safety and security architecture for reducing accidents in intelligent transportation systems. In: Proceedings of the International Conference on Computer-Aided Design, p. 95. ACM (2018)
9. DCSSL: Ebios: Expression of needs and identification of security objectives (2005)
10. De La Torre, G., Rad, P., Choo, K.K.R.: Driverless vehicle security: challenges and future research opportunities. Future Gener. Comput. Syst. (2018)
11. Den Hartog, J., Zannone, N., et al.: Security and privacy for innovative automotive applications: a survey. Comput. Commun. **132**, 17–41 (2018)
12. Dominic, D., Chhawri, S., Eustice, R.M., Ma, D., Weimerskirch, A.: Risk assessment for cooperative automated driving. In: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pp. 47–58. ACM (2016)
13. D'Orey, P.M., Ferreira, M.: ITS for sustainable mobility: a survey on applications and impact assessment tools. IEEE Trans. Intell. Transp. Syst. **15**(2), 477–493 (2014). https://doi.org/10.1109/TITS.2013.2287257

14. Dubois, É., Heymans, P., Mayer, N., Matulevičius, R.: A systematic approach to define the domain of information system security risk management. In: Nurcan, S., Salinesi, C., Souveyet, C., Ralyté, J. (eds.) Intentional Perspectives on Information Systems Engineering, pp. 289–306. Springer, Heidelberg (2010)
15. Engoulou, R.G., Bellaïche, M., Pierre, S., Quintero, A.: VANET security surveys. Comput. Commun. **44**, 1–13 (2014)
16. ENISA: Inventory of risk assessment and risk management methods (2005)
17. Ferreira, M., D'Orey, P.M.: On the impact of virtual traffic lights on carbon emissions mitigation. IEEE Trans. Intell. Transp. Syst. **13**(1), 284–295 (2012)
18. Firesmith, D.: Engineering safety and security-related requirements for software-intensive systems. Carnegie-Mellon University Pittsburg PA Software Engineering Institute, Technical report (2007)
19. Firesmith, D., et al.: Engineering security requirements. J. Object Technol. **2**(1), 53–68 (2003)
20. Fries, R., Chowdhury, M., Brummond, J.: Transportation Infrastructure Security Utilizing Intelligent Transportation Systems. Wiley, Hoboken (2009)
21. Hamida, E., Noura, H., Znaidi, W.: Security of cooperative intelligent transport systems: standards threats analysis and cryptographic countermeasures. Electronics **4**(3), 380–423 (2015)
22. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: VANet security challenges and solutions: a survey. Veh. Commun. **7**, 7–20 (2017)
23. Huang, S., Sadek, A.W., Zhao, Y.: Assessing the mobility and environmental benefits of reservation-based intelligent intersections using an integrated simulator. IEEE Trans. Intell. Transp. Syst. **13**(3), 1201–1214 (2012)
24. Hussain, S., Kamal, A., Ahmad, S., Rasool, G., Iqbal, S.: Threat modelling methodologies: a survey. Sci. Int. (Lahore) **26**(4), 1607–1609 (2014)
25. ISO/IEC: 27001: 2013: Information technology-security techniques-information security management systems-requirements (2013)
26. Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering - a systematic literature review. Inf. Softw. Technol. **51**(1), 7–15 (2009)
27. Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O.P., Turner, M., Niazi, M., Linkman, S.: Systematic literature reviews in software engineering - a tertiary study. Inf. Softw. Technol. **52**(8), 792–805 (2010)
28. Kong, H.K., Hong, M.K., Kim, T.S.: Security risk assessment framework for smart car using the attack tree analysis. J. Ambient Intell. Humanized Comput. **9**(3), 531–551 (2018)
29. Laurendeau, C., Barbeau, M.: Threats to security in DSRC/WAVE. In: Kunz, T., Ravi, S.S. (eds.) ADHOC-NOW 2006. LNCS, vol. 4104, pp. 266–279. Springer, Heidelberg (2006). https://doi.org/10.1007/11814764_22
30. Li, L.: Study on security architecture in the Internet of Things. In: Proceedings of 2012 International Conference on Measurement, Information and Control, vol. 1, pp. 374–377. IEEE (2012)
31. Lu, Y., Maple, C., Sheik, T., Alhagagi, H., Watson, T., Dianati, M., Mouzakitis, A.: Analysis of cyber risk and associated concentration of research (ACR) 2 in the security of vehicular edge clouds. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018, pp. 1–11. IET (2018)
32. Malakorn, K.J., Park, B.: Assessment of mobility, energy, and environment impacts of IntelliDrive-based cooperative adaptive cruise control and intelligent traffic signal control. In: 2010 IEEE International Symposium on Sustainable Systems and Technology (ISSST), pp. 1–6. IEEE, IEEE (2010)

33. Matulevičius, R.: Fundamentals of Secure System Modelling. Springer, Heidelberg (2017)
34. Mejri, M.N., Jalel, B.O., Hamdi, M.: Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)
35. Moalla, R., Labiod, H., Lonc, B., Simoni, N.: Risk analysis study of its communication architecture. In: 2012 3rd International Conference on the Network of the Future (NOF), pp. 1–5. IEEE (2012)
36. Morris, B.T., Tran, C., Scora, G., Trivedi, M.M., Barth, M.J.: Real-time video-based traffic measurement and visualization system for energy/emissions. IEEE Trans. Intell. Transp. Syst. **13**(4), 1667–1678 (2012)
37. Mukisa, S.S., Rashid, A.: Cyber-security challenges of agent technology in intelligent transportation systems. In: Proceedings of the 1st International Workshop on Agents and CyberSecurity, p. 9. ACM (2014)
38. ben Othmane, L., Ranchal, R., Fernando, R., Bhargava, B., Bodden, E.: Incorporating attacker capabilities in risk estimation and mitigation. Comput. Secur. **51**, 41–61 (2015)
39. OWASP: Top 10 IoT Vulnerabilities (2014)
40. Pelzl, J., Wolf, M., Wollinger, T.: Automotive embedded systems applications and platform embedded security requirements. In: Markantonakis, K., Mayes, K. (eds.) Secure Smart Embedded Devices, Platforms and Applications, pp. 287–309. Springer, New York (2014). https://doi.org/10.1007/978-1-4614-7915-4_12
41. Perallos, A., Hernandez-Jayo, U., Zuazola, I.J.G., Onieva, E.: Intelligent Transport Systems: Technologies and Applications. Wiley, Hoboken (2015)
42. Ruddle, A.R., Ward, D.D., Perallos, A., Hernandez-Jayo, U., Onieva, E., Garcıa-Zuazola, I.: Cyber security risk analysis for intelligent transport systems and in-vehicle networks. In: Intelligent Transport Systems Technologies and Applications, p. 83 (2015)
43. Servin, O., Boriboonsomsin, K., Barth, M.: An energy and emissions impact evaluation of intelligent speed adaptation. In: 2006 IEEE Intelligent Transportation Systems Conference, ITSC 2006, pp. 1257–1262. IEEE (2006)
44. Shostack, A.: Threat Modeling: Designing for Security. Wiley, Hoboken (2014)
45. Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J., Xiong, Y., Cui, X.: Attacks and countermeasures in the internet of vehicles. Ann. Telecommun. **72**(5–6), 283–295 (2017)
46. Tao, C.C.: Dynamic taxi-sharing service using intelligent transportation system technologies. In: 2007 International Conference on Wireless Communications, Networking and Mobile Computing, WiCom 2007, pp. 3209–3212. IEEE (2007)
47. Tbatou, S., Ramrami, A., Tabii, Y.: Security of communications in connected cars modeling and safety assessment. In: Proceedings of the 2nd International Conference on Big Data, Cloud and Applications, p. 56. ACM (2017)
48. Tielert, T., Killat, M., Hartenstein, H., Luz, R., Hausberger, S., Benz, T.: The impact of traffic-light-to-vehicle communication on fuel consumption and emissions. In: 2010 Internet of Things (IOT), pp. 1–8. IEEE (2010)
49. Tsugawa, S., Kato, S., Aoki, K.: An automated truck platoon for energy saving. In: 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 4109–4114. IEEE (2011)
50. Wohlin, C.: Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th International Conference on Evaluation And Assessment in Software Engineering, p. 38. ACM (2014)

51. Yang, X., Li, Z., Geng, Z., Zhang, H.: A multi-layer security model for Internet of Things. In: Wang, Y., Zhang, X. (eds.) IOT 2012. CCIS, vol. 312, pp. 388–393. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32427-7_54
52. Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W.: Study and application on the architecture and key technologies for IoT. In: 2011 International Conference on Multimedia Technology, pp. 747–751. IEEE (2011)
53. Yousuf, O., Mir, R.N.: A survey on the Internet of Things security: state-of-art, architecture, issues and countermeasures. Inf. Comput. Secur. **27**(2), 292–323 (2019)
54. Zhang, Z., Cho, M.C.Y., Wang, C., Hsu, C., Chen, C., Shieh, S.: IoT security: ongoing challenges and research opportunities. In: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234 (2014)
55. Zhao, K., Ge, L.: A Survey on the Internet of Things security. In: 2013 9th International Conference on Computational Intelligence and Security, pp. 663–667. IEEE (2013)
56. Zhou, H., Liu, B., Wang, D.: Design and research of urban intelligent transportation system based on the Internet of Things. In: Wang, Y., Zhang, X. (eds.) IOT 2012. CCIS, vol. 312, pp. 572–580. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32427-7_82