Security in V2I Communications

Subjects: Computer Science, Theory & Methods | Telecommunications

Contributor: Pablo Marcillo, Diego Tamayo-Urgilés, Ángel Leonardo Valdivieso Caraguay, Myriam Hernández-Álvarez

The number of vehicles equipped with wireless connections has increased considerably. The impact of that growth in areas such as telecommunications, infotainment, and automatic driving is enormous. More and more drivers want to be part of a vehicular network, despite the implications or risks that, for instance, the openness of wireless communications, its dynamic topology, and its considerable size may bring. Undoubtedly, this trend is because of the benefits the vehicular network can offer. Generally, a vehicular network has two modes of communication (V2I and V2V). The advantage of V2I over V2V is roadside units' high computational and transmission power, which assures the functioning of early warning and driving guidance services. Researchers have identified the non-resistance to attacks, the regular updating and exposure of keys, and the high dependence on certification authorities as main vulnerabilities.

Keywords: VANET ; V2I ; security ; privacy ; authentication ; confidentiality ; integrity

1. Introduction

According to Statista [1], by 2021, the number of connected vehicles worldwide will reach 237 million units, and by 2025 that number will be 400 million. The impact of those numbers in the telecommunication area is enormous. One of the implications is related to security in communications. Because of the opening of wireless communications, the dynamic topology and the big size of the network, and the use of the same credentials for registration, attackers may be able to listen, forge, manipulate, or destroy information exchanged between vehicles and roadside units affecting the proper operation and performance of the network [2][3][4].

Generally, there are two modes of communication in a vehicular network: Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V). This last one has the advantage of having roadside units (RSU) with high computational and transmission power to exchange information at high speed with vehicles. For instance, it assures the correct operation of driving guidance and early warning services. In addition to the advantages of V2I, benefits such as avoiding traffic accidents or traffic jams or accessing services on the Internet could justify why many authors have focused more on V2I communication than V2V [2][3]. In that way, it is also essential to cover some aspects of security in this type of communication.

This entry aims to report the most current and relevant information on V2I communications security. In that way, the authors posed five research questions. The first one is related to the vulnerabilities in this type of communication and their respective countermeasures. The second concerns the methods, technologies, tools, or mechanisms used to provide security solutions to mitigate these vulnerabilities. The third and fourth ones are about the available evaluation metrics to measure the effectiveness of the solutions and thus find out which offers the best results. Finally, the last one concerns the challenges to be faced by the proposals and their possible solutions.

One of the contributions of the present entry is the information that the authors provided compared to previous studies related to the same topic. The authors noted that almost all reviews focus on all communication in Vehicular Ad-hoc Network (VANET) without emphasizing V2I communication. VANET is a large overall system model comprising four approaches comprehending driver and vehicle, traffic flow, communications, and applications. The components related to data communication are V2V and V2I. The whole system is vast and complex. Therefore, this research aims to provide a systematic literature review centered on one of the components of VANET: V2I communication, to review it in more detail.

2. Concepts and Definitions of V2I

2.1. Security Requirements

- Confidentiality: It guarantees that only authorized nodes can access and reveal sensitive information.

- Integrity: It ensures that the information sent by the sender is the same as that received by the receiver.

- Authentication: It guarantees that the node that wants to access or use network resources is who it claims to be.

- Availability: It ensures that the access to network resources for authorized nodes is continuous and without interruptions.

- Non-repudiation: It guarantees that neither the receiver nor the sender can deny having processed certain information.

2.2. Attacks

- MitM: It occurs when an adversary secretly enters the communication of two devices to make them believe that they are communicating directly and thus exchange its public key between the devices.

- Replay: It occurs when an adversary listens to the communication, intercepts it, and later fraudulently resend the obtained messages.

- Modification/Tampering: It occurs when an adversary alters the message transmitted between two nodes fraudulently.

- DoS: It occurs when an adversary floods the communication system with no genuine requests getting the service down.

- Repudiation: It occurs when a system or application does not track nor log the user’s actions properly, permitting manipulation or forging new actions.

- Session Key Disclosure: It occurs when an adversary can obtain values from memory devices (OBU or TPD) and messages from insecure communication channels. Thus, the adversary can calculate the session key using the values and messages.

- Impersonation: It occurs when an adversary can take someone’s identity to gain advantages or cause damage to other nodes.

- Sybil: It occurs when an adversary forges node identities to obtain privileges and thus causes chaos in normal conditions.

- Forgery: It occurs when an adversary forges a valid certificate and signs a message successfully.

- Bogus: It occurs when an adversary generates a fake node in a network and informs it about false traffic conditions in a particular location.

- Eavesdropping: It occurs when an adversary listens to the communication channel extracting information that can be useful for node tracking activity.

- Plaintext: It occurs when an adversary, who has access to the ciphertext and its plaintext, tries to guess the secret key or develops an algorithm for decrypting messages.

- Key Leakage: It occurs when an adversary, who has access to the signer, can learn some sensitive information (e.g., computation-time, memory contents, and others).

- Chosen Message: It occurs when an adversary, who can obtain the ciphertext of plaintext messages from the signer, tries to reveal the secret encryption key.

- Ciphertext: It occurs when an adversary, who has access to a set of ciphertexts, tries to guess the plaintexts or even the key.

- Beacon Transmission Denial: It occurs when an adversary suspends itself its beacon transmission for an indefinite time to avoid detection.

2.3. Evaluation Metrics

- Computational Cost: It refers to the time required to apply certain operations to a message before sending it over the network.

- Communication Overhead: It refers to the length of information transmitted by a successful message transference.

- Transmission Delay: It refers to the time a packet takes to get to the destination from the source.

- Propagation Delay: It refers to the distance between the sender and receiver divided by the light speed.

- Packet Delivery Ratio: It refers to the ratio of packets successfully delivered to their destinations.

- Packet Loss Ratio: It refers to the ratio between the number of lost packets and the total number of sent packets.

- Accuracy: It refers to the general ratio of vehicles correctly detected.

- Trust Value: It refers to the general cooperativeness of a user.

- Data Receiving Rate: It refers to the rate of data successfully received.

- Storage Cost: It refers to the memory size required to store the parameters in the different devices.

- Roaming Latency: It refers to the time required to transfer the node control between gateways.

- Cyphertext Length: It refers to the length of messages after performing encryption operations.

- Energy Consumption: It refers to the energy consumed during the routing process.

- Throughput: It refers to the rate of messages successfully transmitted in one second over a communication channel.

- Attack Detection Ratio: It refers to the ratio between the number of attacks detected and the total number of attacks.

- Average Delay: It refers to the expected time a beacon message of a node remains in a queue before being sent to the infrastructure.

- False Accept Ratio: It refers to the ratio between the correct number of planned trajectories and the total number of trajectories of a node.

2.4. Methods

- Elliptic Curve Cryptography (ECC): It is a public key encryption technique that generates cryptographic keys using the elliptic curve theory.

- Public Key Cryptography (PKC): It is a scheme that performs encryption and decryption using public and private keys. The public key is published, and the private one is kept secret. It is known as asymmetric key cryptography.

- Symmetric Key Cryptography (SKC): It is a cryptography scheme that uses the same key for encryption and decryption.

- Public Key Infrastructure (PKI): It is a scheme in which the public key is associated with a certificate provided by a certificate authority instead of choosing one generated randomly.

- Identity-Based Public Key Cryptography (IBPKC): It is a scheme that uses a representation of identity as the public key to avoid using public ones associated with a certificate. Instead of a certificate authority, there is a key generation center to generate the private keys based on the public ones.

- Certificateless-Based Cryptography (CBC): It is a scheme that distributes the private keys of the key generation center into several entities. In this scheme, the user and the key generation center calculate the private key, but only the user can obtain the result.

3. Research Questions on V2I

The answers to the five research questions are presented as follows.

RQ01: What are the principal vulnerabilities in V2I communications?

Since wireless communications are easy to intercept, the principal vulnerability in this type of communication is the susceptibility to attacks. Thus, adversaries can compromise RSUs/vehicles and send false information to drivers putting their lives at risk. They can also send unnecessary alerts to distract them and control the communication links. Once it is done, the adversaries can easily modify session messages. Considering that fact, researchers have focused on proposing solutions that offer any attack resistance. From the results, the authors identified the attacks to which the solutions are resistant. They found the following attacks: MitM, Replay, Tampering, DoS, Repudiation, Session Key Disclosure, Impersonation, Sybil, Forgery, Eavesdropping, and Plaintext. The authors commonly offer solutions against Replay, Impersonation, MitM, Tampering, and Sybil attacks.

RQ02: What methods, technologies, or tools can mitigate those vulnerabilities?

The proposals were grouped using the following categories. The Network Communication Security category for routing protocols, communication schemes, messages exchange security, and privacy protection; the Malicious Node Detection category for intrusion detection systems, trust management schemes, and intrusion prevention systems; and the Authentication Scheme category. According to **Figure 1**, eight of every ten proposals are about Authentication Schemes, one is about Network Communication Security, and less than one is about Malicious Node Detection.

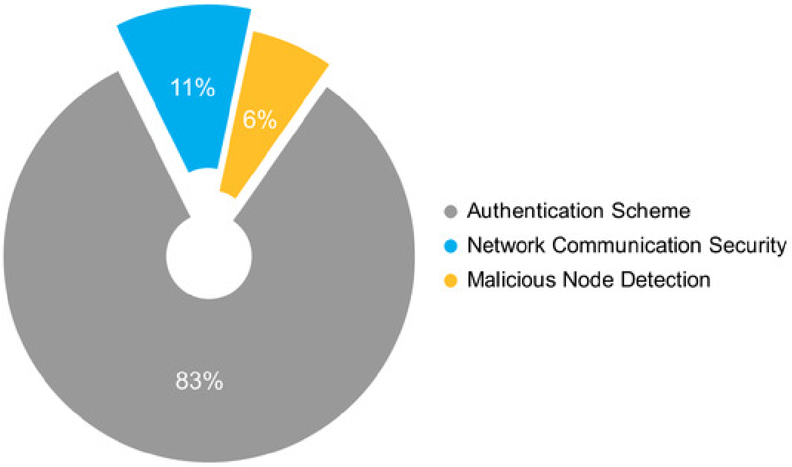

Figure 1. Types of solutions based on the frequency of occurrence.

Regarding technologies, The authors observed that there are several solutions based on PKC/ECC with Blockchain. This technology is gaining attentions in various study fields. This interest must be due to its key features such as decentralization, anonymity, and immutability [5][6]. Regarding simulators, authors have used both network and traffic ones. **Figure 2** presents the use of simulators in studies based on the frequency of occurrence. According to it, they use OMNeT++, NS-3, and NS-2 to a greater extent and Veins, SSGA, and MOVE to a lesser extent, and the only traffic simulator is SUMO.

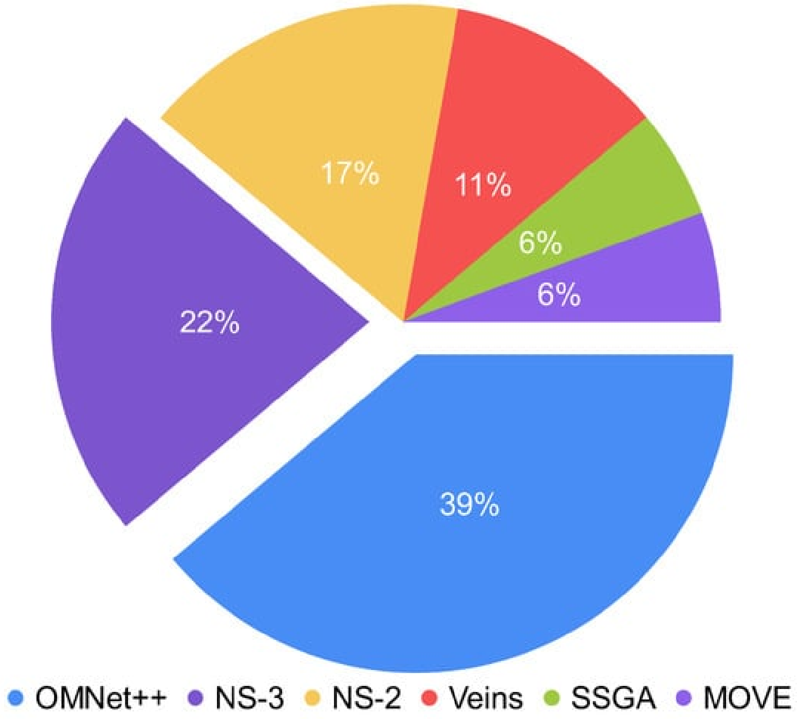

Figure 2. Use of network simulators based on the frequency of occurrence.

RQ03: What evaluation metrics are available to measure the effectiveness of those methods or tools?

Researchers have used the following evaluation metrics to measure the performance of their solutions. Metrics such as computational cost/time/overhead, communication cost/overhead, storage cost/overhead, transmission delay, propagation delay, packet delivery ratio, packet drop ratio, accuracy, trust value, data receiving rate, roaming latency, cyphertext length, energy consumption, and false success rate. The more common metrics in order of occurrence are computational cost, communication overhead, transmission delay, and packet delivery rate. Because of the use of emerging technologies to solve certain obstacles and limitations, more researchers are focusing on evaluation metrics such as computational cost and communication overhead to measure the effectiveness of their solutions.

RQ04: What methods, technologies, or tools provide the best results based on those evaluation metrics?

From the results, the authors could establish that the solutions that offer better results are the ones in which the use of emerging technologies to overcome certain limits and obstacles are present. Thus, considering metrics such as computational cost and overhead, the solutions based on Fog/Edge/Cloud computing present better results than the others. The following comparative analysis (**Table 1**) reinforces this assumption.

Table 1. Comparative analysis of emerging technologies in relation to some performance metrics.

	Blockchain	**Fog Computing**	**Edge**	**Cloud**	**Cloudlets**
Latency	**Low**	**Medium**	**Low**	**High**	**Low**
Scalibility	**Low**	**High**	**High**	**Medium**	**Low**
Energy Consumption	**High**	**Medium**	**Low**	**High**	**Medium**
Interoperability	**Low**	**High**	**Low**	**High**	**Low**

From the main methods (**Figure 3**), there is a slight trend of using Elliptic Curve Cryptography (ECC) instead of traditional cryptography (PKC); however, the evaluation metrics present good results for both cases. In this case, it is necessary for further research to determine the best method based on the evaluation metrics. Apart from the methods, researchers have also used network and traffic simulators, map tools, security tools, programming languages, platforms, and libraries. **Figure 4** presents the distribution of the tools used in the proposals. The most used map tool is Open Street. About security tools, the most common are MIRACL and Avispa. The most used programming languages are C and Python, and among libraries, OpenSSL.

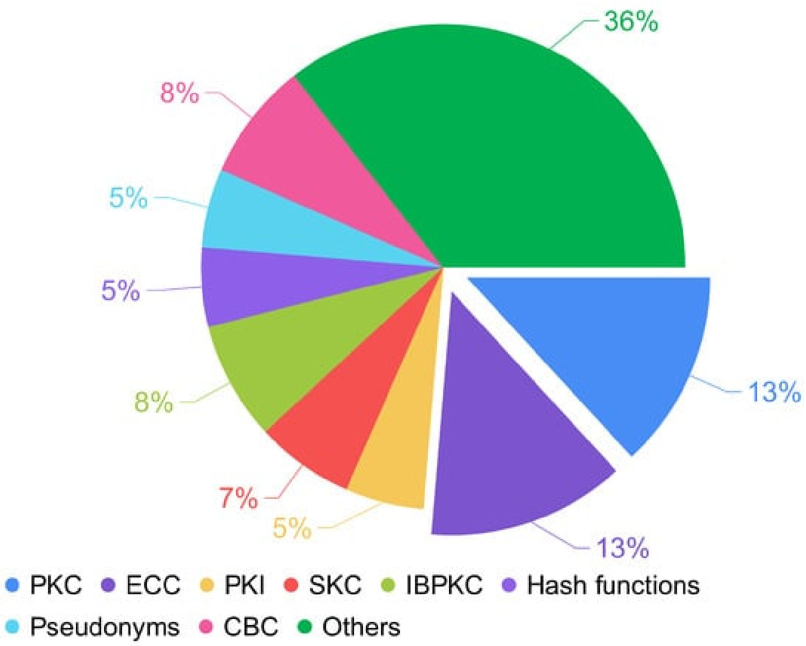

Figure 3. Use of methods based on the frequency of occurrence.

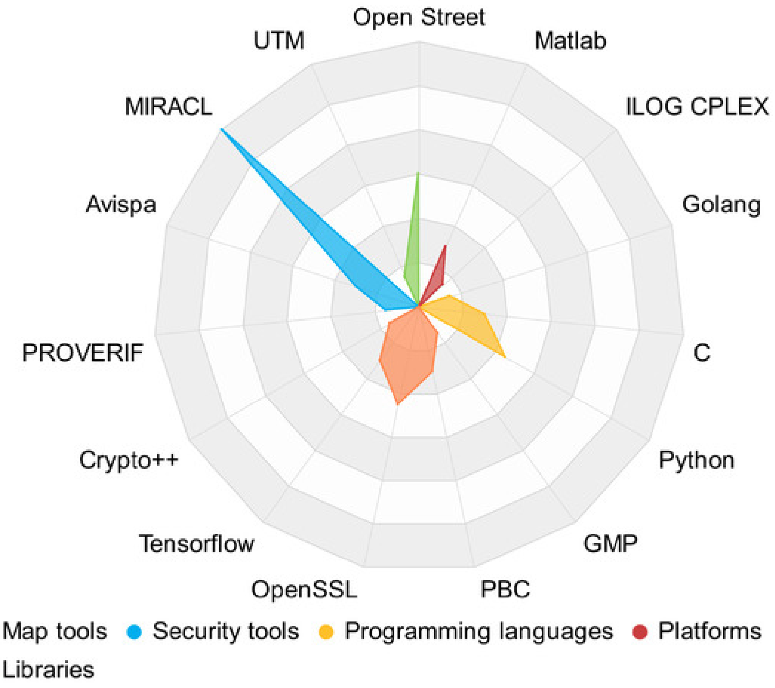

Figure 4. Use of tools based on the frequency of occurrence.

RQ05: What are the principal challenges for mitigating vulnerabilities in VANETs?

Since vehicles with limited computing resources must interact with communication infrastructure at high speed, the great challenge in vehicular networks is to dispose of a safe and reliable communication channel and suitable device performance. When a vehicle enters the coverage of a new roadside unit, the computational overhead can lower the quality of communications and driving safety. Not all attacks in vehicular networks are protected with security mechanisms such as cryptography techniques, digital signatures, or message verification technique, and there are others as the bogus attack that requires a solution. Counting with a secure channel to transmit authentication information is still a paradigm considering that some security schemes must be applied to resource-limited and time-critical devices.

4. Conclusions and Future Work

The capacity of modern vehicles to connect to an external infrastructure makes them vulnerable to cyber-attacks. Counting with a secure channel to transmit authentication information is still a paradigm considering that some security schemes must be applied to resource-limited and time-critical devices. V2I communications offer more advantages and benefits to users than V2V communications. Hence, the reasons for studying the state-of-the-art of security in V2I communications.

In the present entry, the authors found that the principal attacks to which solutions are resistant are multiple and varied. The attackers could intrude on a network to intercept and manipulate the messages using MitM, Replay, Repudiation, Eavesdropping, or Tampering; shut down a machine making it inaccessible with DoS; pretend to be someone else to access information through impersonation and Sybil attack; tricks a web browser into executing unwanted actions using Forgery; obtain the key with plaintext attacks where the attacker knows the plaintext and its corresponding encrypted ciphertext or with Exploitation of the session control mechanisms with Session Key disclosure; among others fraudulent techniques.

Diverse methods and tools are developed to mitigate these vulnerabilities. They grouped them into solutions for authentication/trust management/network communication schemes for privacy preserving, IDS and IPS models to alert and act over a security incident, and routing protocol management to protect the devices. To evaluate the effectiveness of the methods and tools used to mitigate the vulnerabilities that measure computational cost through communication overhead, transmission delay, and data delivery reliability. The authors observed that researchers must address their future work toward using emerging technologies to reduce computational overhead and save computational costs. They observed a slight trend in using ECC instead of traditional cryptography. However, it is too soon to establish if ECC will become the dominant choice in cryptography in a few years. What is certain is that the use of emerging technologies such as Fog/Edge/Cloud computing, Cloudlets, Blockchain, Software-Defined Networking, and Network Functions Virtualization has suffered a rapid expansion. In fact, the inclusion of emerging technologies in proposals has contributed to reducing the computational overhead and saving the computational costs.

After conducting a simplified review of reviews, the authors observed that the number of analyzed articles in almost all reviews is insufficient, and the lack of a search strategy is surprising. The reviews vaguely mentioned evaluation metrics and emerging technologies as possible solutions to overcome certain limitations. Concerning the methods used to build solutions, the other authors mentioned at least the most common ones. Finally, the list of threats/attacks proposed in the reviews is relatively small compared to the list in the present entry.

On the other hand, the authors identified coincidences in the presentation of information on fundamentals, security requirements, threats/attacks, solutions, and challenges. However, the present entry stands out because it presents, for instance, a comparative analysis of emerging technologies in relation to some performance metrics, some graphics related to the percentage of occurrence in solutions of the methods, tools, and simulators used by researchers to build solutions against vulnerabilities, and also one representing the percentage of occurrence about the types of solutions presented in the present entry. Not to mention the valuable information the authors obtained from a review of review articles.

References

1. Placek, M. Connected Cars Worldwide-Statistics & Facts. Available online: https://www.statista.com/topics/1918/connected-cars/ (accessed on 30 October 2022).
2. Zhou, F.; Li, Y.; Ding, Y. Practical V2I Secure Communication Schemes for Heterogeneous VANETs. Appl. Sci. 2019, 9, 3131.
3. Park, Y.; Sur, C.; Rhee, K.H. Pseudonymous authentication for secure V2I services in cloud-based vehicular networks. J. Ambient. Intell. Humaniz. Comput. 2016, 7, 661–671.
4. Abassi, R. VANET security and forensics: Challenges and opportunities. Wiley Interdiscip. Rev. Forensic Sci. 2019, 1, e1324.
5. Pradhan, N.R.; Singh, A.P.; Verma, S.; Wozniak, M.; Shafi, J.; Ijaz, M.F. A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. Sci. Rep. 2022, 12, 1–15.
6. Wadhwa, S.; Rani, S.; Verma, S.; Shafi, J.; Wozniak, M. Energy Efficient Consensus Approach of Blockchain for IoT Networks with Edge Computing. Sensors 2022, 22, 3733.