Human Factors in Cybersecurity, Vol. 53, 2022, 128–137
https://doi.org/10.54941/ahfe1002210

Security in Vehicle-to-Infrastructure Communications

Pablo Marcillo, Ángel Leonardo Valdivieso Caraguay, and Myriam Hernández-Álvarez

Departamento de Informática y Ciencias de la Computación, Escuela Politécnica Nacional, Ladrón de Guevara E11-25 y Andalucía, Edificio de Sistemas, 170525, Quito, Ecuador

ABSTRACT

By 2020, the number of connected vehicles will reach 250 million units. Thus, one of five vehicles worldwide will count on any wireless connection. Functional areas such as telecommunications, infotainment, automatic driving, or mobility services will have to face the implications caused by that growth. As long as vehicles require exchanging information with other vehicles or accessing external networks through a communication infrastructure, these vehicles must be part of a network. A VANET is a type of mobile network formed by base stations known as Road Side Units (RSU) and vehicles equipped with communication units known as Onboard Units (OBU). The two modes of communication in a VANET are Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Some authors consider that V2I communication has more advantages than V2V communication because V2I communication provides services such as driving guidance or early warning for drivers. This consideration has meant that researchers show more interest in this mode of communication. Likewise, others affirm that the problem of V2I communication is its security. This review focuses on knowing the most relevant and current approaches on security in V2I communication. Among the solutions, we have authentication schemes based on Blockchain technology, Elliptic Curve cryptography, key insulation strategy, and certificateless aggregate signature technique. Also, we found security architectures and identification schemes based on SDN, NFV, and Fog/Edge/Cloud computing. The proposals focus on resolving issues such as the privacy-preserving, high computational work, regular updating and exposure of secret keys, large number of revoked pseudonyms lists, lack of scalability in networks, and high dependence on certification authorities. In addition, these proposals provide countermeasures or strategies against replay, message forgery, impersonation, eavesdropping, DDoS, fake information, modification, Sybil, man-in-the-middle, and spoofing attacks. Finally, we determined that the attacks in V2I communications mostly compromise security requirements such as confidentiality, integrity, authentication, and availability. Preserving privacy by reducing computational costs by integrating emerging technologies is the direction toward security in vehicular network points.

Keywords: VANET, V2I, Security, Privacy, Authentication

INTRODUCTION

By 2020, one of five vehicles worldwide will be equipped with any wireless connection (Gartner). In real terms, there will be more than 250 million connected vehicles. Therefore, there will be significant growth of drivers at their disposal in-vehicle services and automated driving capabilities. The implications of that growth in areas such as telecommunications, infotainment, and mobility services will be enormous. One of these implications is related to security in communications, particularly in vehicular networks.

In general terms, the two modes of communication into a VANET are V2V and V2I. The major advantage of V2I over V2V is the high speed at which information is broadcasted to vehicles through RSUs (Zhou, Li, & Ding, 2019). It is due to the high computational power and the ability of broadcasting of RSUs, whereby the correct operation of driving guidance or early warning services may be assured. At present, vehicles through RSUs can avoid traffic accidents or traffic jams and access services on the Internet (Park, Sur, & Rhee, 2016).

Because of the opening of wireless communications, the dynamic topology of VANETs (constant motion of vehicles and short connection times), the big size of the network, and the use of the same user credentials for registration into every RSU, attackers can be able to listen, forge, and destroy information exchanged between vehicles or RSUs affecting the proper operation and the performance of the network, without forgetting the impact on security requirements (Zhou, Li, & Ding, 2019) (Park, Sur, & Rhee, 2016) (Abassi, 2019).

There are some techniques or measures to deal with attacks that affect some security requirements. In general, the digital signature can be used to assure integrity, authentication, and non-repudiation; and encryption to assure confidentiality (Zhou, Li, & Ding, 2019) (Manvi & Tangade, 2017). With more detail and according to (Kumar, Bansal, & others, 2017), ciphers can be used against eavesdropping attack, time-stamping technique against the replay attack, the integration of a CA or the use of a Public Key Infrastructure (PKI) against the node impersonation attack, and IP information handling against DoS attacks.

This paper introduces a review on security in V2I communications. This study aims to know about the solutions, their main features, the technology used, security aspects solved, the attacks to which they are resistant or to which they provide protection, and the security requirements compromised by attacks. To this effect, and to fulfill the objective of this work, we posed three research questions.

We organized the rest of the article as follows. Section 2 introduces a revision on VANETs, security requirements, and attacks focused on V2I communication. Section 3 presents the methodology used in this study, followed by Section 4, which gives the most relevant and current aspects related to security in V2I communications. Then, Section 5 presents the results obtained from this study. Finally, Section 6 presents the conclusions of this research work.

OVERVIEW

Vanets

A VANET is a mobile ad-hoc network integrated by vehicles, a type of radio base called Road Side Unit (RSU), and a Certificate Authority (CA). It is known that there two modes of communication in VANET. The first one is called Vehicle to Infrastructure (V2I) where vehicles equipped with Onboard Units (OBU) send and receive information from and to RSU; and the second one called Vehicle to Vehicle (V2V) where vehicles send and receive information from each other directly and without the help of infrastructure in the middle. Even at present, some authors have proposed and adopted the Vehicle to Everything (V2X). V2X covers the common modes of communication such as V2I and V2V, and new ones such as Vehicle to Pedestrian (V2P), Vehicle to Network (V2N), and Vehicle to Grid (V2G).

Regarding V2I communication, it generally involves access to external networks such as the Internet or cloud services (Chen, et al., 2017) (Boukerche & Robson, 2018). At present, the concept of vehicular cloud computing has been established to show the need for vehicular networks to be supported by cloud computing services (Park, Sur, & Rhee, 2016). Two of the most popular services are Intelligent Transportation System (ITS) for safe driving and Telematics for entertainment and location. In that way, and depending on the type of application / service, additional computational power and storage will be essential to process a large amount of information.

Security Requirements

Considering that V2I communication has more advantages than V2V communication because V2I communication provides services such as driving guidance or early warning for drivers, this mode of communication has captured the researcher's attention. According to (Zhou, Li, & Ding, 2019), a critical problem of V2I communication is its security. In fact, some authors (Ali, Gervais, Ahene, & Li, 2019) consider the authentication of messages exchanged between vehicles and RSUs as one of the most important security requirements. In that way, some security requirements must be covered to improve security in V2I communications. Those requirements are presented as follows.

- Confidentiality ensures that only authorized nodes can read the information.
- Integrity guarantees the information is the same on the sender and receiver sides.
- Authentication guarantees that the node is what it claims to be.
- Availability guarantees access to any resource network by authorized nodes is continuous and without interruptions.
- Non-repudiation ensures that a node is able and not denied to transmit messages.

Attacks

The following attacks occur in V2I communication.

- Eavesdropping: The attacker sniffs the network communications to intercept sensitive information.
- Tampering: The attacker captures the messages exchanged in communications, modify, and forward them.

- Replay: The attacker intercepts communications to capture messages to forward several times or delay them.
- DoS: The attacker makes a network resource inaccessible temporarily or indefinitely to its users.
- Impersonation: The attacker assumes the identity of a trusted entity into a communication protocol to intercept sensitive information.
- Malware: An intrusive software designed to steal information or damage systems.
- Spam: Any not requested form of communication sent massively.

There are two attack methods: passive and active. In the passive method, the attacker only listens to information exchanged between nodes (vehicles or RSUs), while in the active method, the attacker may falsify, modify and destroy that information (Abassi, 2019) (Ayoub & Mazri, 2018). The consequences of attacks will greatly depend on the attacker's profile. For instance, the attack performed by a malicious attacker will be more harmful than by a rational attacker.

Some authors propose a taxonomy to classify attacks (Abassi, 2019) (Islam, Chowdhury, Li, & Hu, 2018) (Elsadig & Fadlalla, 2016) (Kaur, Singh, & Khajuria, 2018). We created a new one but focused on V2I communications. As follows, we present a summary of the categories defined for this taxonomy.

- Monitoring: Attacks that perform listening and tracking activities over the communications.
- Network: Attacks that involve affectations and restrictions in the communication networks.
- Application: Attacks that affect applications focused on providing services in vehicular networks.

METHODS

This work presents the state of the art on security in V2I communications. The articles were selected considering the inclusion criteria presented as follows. Only papers published in the last five years, written in English, published in journals and conferences, and also that responded directly with the following questions:

- What are the most relevant and current on security in VANET for V2I communications?
- What are the main vulnerabilities or attacks in V2I communications?
- What are the countermeasures against those vulnerabilities or attacks?

The citation databases used in this work were Scopus, IEEExplore, and Google Scholar. The most relevant and current security aspects in V2I communications are introduced as follows. Based on the research questions, we extracted the following keywords: VANET, V2I, security, vulnerabilities, and countermeasures. Also, we added the meaning of the acronyms VANET and V2I. We developed a search string combining the keywords with the operator AND and OR.

RELATED WORK

The proposals generally focus on improving certain aspects of the existing authentication protocols and security schemes by providing innovative concepts, strategies, or mechanisms. Below, we present the most relevant and current proposals.

- *Security based on signature-then-encryption*: (Zhou, Li, & Ding, 2019) propose four security schemes for V2I communications based on the signature-then-encryption method. Two of them allow secure communication between many vehicles and one RSU registered in PKI or IBC (Identity-Based Cryptosystem) systems. Meanwhile, the other two schemes allow the broadcasting of one message to many vehicles from one RSU registered in PKI/IBC systems.
- *Security based on blockchain*: (Zheng, Jing, Guo, Gao, & Wang, 2019) present a framework, which provides a decentralized and trustworthy communication environment by providing an authentication schema that decreases the dependency on CA, provides an audit of malicious vehicles, and accomplishes privacy protection of vehicles. Also, they propose a storage scheme based on distributed cloud and blockchain technologies, which stores announcement transactions of vehicles.
- *Non-use of batch verification method*: (Al-Shareeda, Anbar, Alazzawi, & Manickam, 2020) suggest an authentication scheme to verify many messages simultaneously without the use of the common batch verification method. It is known that the use of that method causes computational overhead. Instead, this scheme uses an optimized verification method, the Elliptic Curve Cryptography (ECC) algorithm for authentication and XOR and hash functions for the broadcasting process.
- *Certificateless public key signature*: (Ali, Gervais, Ahene, & Li, 2019) present a public key signature scheme without certificates for V2I communication. This scheme uses bilinear pairing to provide conditional authentication; supports batch verification signature function to verify multiple signatures at the same time; aggregate verification signature function to improve the communication bandwidth between RSUs and Traffic Control Centers (TFC), and includes blockchain technology to implement transparency in revocation of pseudonymous.
- *Trustworthiness scalable computation*: (Wang, Shen, Lai, & Liu, 2020) propose an authentication scheme for V2I communication based on blockchain technology. This scheme uses blockchain to record vehicle attributes and trustworthiness, which will be checked later in search of changes; trustworthiness computation to ensure the reliability of vehicles previously authenticated, and Merkle hash tree (MHT) to record vehicle attributes in real-time. Also, this scheme offers an additional authentication phase to make sure the exchange of the ownership vehicles among RSUs, which provides scalability to the network.
- *Pseudonymous access tokens*: (Park, Sur, & Rhee, 2016) suggest an anonymous cloud access management system for V2I communication. This system is based on pseudonymous access tokens for vehicles, which make

use of pseudonymous and cryptography primitives based on identity, and a revocation mechanism for RSUs to decrease the size of revocation lists. Thus, only a part of the revoked pseudonymous list and not the whole list is distributed to RSUs.

- *Authentication based on key insulation*: (Zhou, Liu, Xiao, Deng, & Wang, 2018) propose an authentication scheme in which the private key of the vehicle, used to authenticate into VANET, is divided into two parts: one part managed by the vehicle and the other by a tamper-proofing device (TPD). The part of the key managed by TPD is constantly updated, and then it is joined to the part managed by the vehicle to generate a signature, which is validated later by the RSU.
- *Certificateless aggregate signature*: (Zhong, Han, Cui, Zhang, & Xu, 2019) suggest a privacy-preserving authentication scheme based on the certificateless aggregate signature technique to message signing. This scheme proposes to reduce the computational cost and communication and storage overhead. In that way, pseudonyms are used to accomplish conditional privacy-preserving; and a trace authority (TA) is in charge of the generation of pseudonyms and the tracking to trace the real identity of vehicles during the communication.
- *Rogue vehicle detection based on Fog computing*: (Al-Otaibi, Al-Nabhan, & Tian, 2019) present a privacy-preserving scheme in which traffic data sharing is only allowed through RSUs (fog nodes) but not between vehicles (end-users). This mechanism permits the identification of vehicles that provide false traffic data and the elimination of them from the VANET. In this scenario, RSUs and not vehicles accomplish the calculation of the road situation; therefore, the vehicles reduce their computational overhead drastically.
- *Security based on emerging technologies*: (Islam, Chowdhury, Li, & Hu, 2018) propose a security architecture for V2I applications called CVGuard. This architecture is conceived as a distributed computing platform based on emerging technologies such as edge computing, SDN (Software-Defined Networking), and NFV (Network Functions Virtualization); and focused on security at the network level. Also, it can provide countermeasures against threats and protection and prevention for applications compromised by cyber-attacks.
- *Continuous key exchange protocol*: (Palaniswamy, et al., 2020) suggest a driver authentication protocol and a key exchange protocol for V2I. The first protocol provides conditional anonymity and unlinking of vehicles. Also, it is resistant to replay, masquerading, password guessing, and lost smart verifier card attacks. The second one guarantees continuous authentication of a vehicle when entering and exiting from one RSU to another by providing the handoff capability.
- *Authenticated key agreement scheme*: (Wei, Cui, Zhong, Xu, & Liu, 2021) propose a scheme based on elliptic curve cryptography and hash functions. The scheme consists of a three-party authentication protocol and key agreement algorithm to simultaneously secure communication channels

(V2I and V2V). The protocol permits mutual authentication among vehicles, RSUs, and TAs. Meanwhile, the algorithm provides computation of common session keys and support for vehicle entry and exit operations.

- *Cloudlet supported secure communication*: (Gupta, Benson, Patwa, & Sandhu, 2020) suggest a mechanism to authorize, check, and verify messages exchanged among moving entities using trusted cloudlets. This mechanism is based on the concept of dynamic edge associations in which the entities connect to cloudlets installed on the road. The development of security policies at cloudlets ensures that these can block fake messages and provide trustworthiness. Since the messages come through cloudlets and these can anonymize messages, it is impossible to determine the identity of the transmitter, so user privacy is guaranteed.
- *Privacy-Preserving authentication protocol*: (Lv & Liu, 2021) propose a protocol that uses BGN homomorphic encryption. This protocol obtains information from all RSUs located on the travel route before the trip. This information is used during the travel to ensure a fast authentication at the moment to enter the coverage of any RSU. In addition, this protocol guarantees the route plan privacy because the Certification Authority (CA) does not know the information from the previously deduced RSUs.
- *Handover authentication protocol based on blockchain*: (Son, Lee, Park, Park, & Das, 2022) present an authentication protocol that starts with a setup phase. In this phase, a trace authority publishes parameters for communication and configures RSUs. Then, the vehicles are registered with the trace authority to authenticate and communicate with nearby RSUs. Once the vehicle is authenticated with an RSU, the blockchain loads its authentication information. The authentication with the next RSU will be made only using hash and XOR operations. In case of RSU discovers misbehavior of a vehicle, it could revoke the vehicle from the blockchain without the support of trace authority.
- *Authentication based on symmetric cryptography and group key distribution*: (Liu, Guo, Zhong, & Yao, 2017) propose an authentication protocol designed with symmetric cryptography and group key distribution. It consists of the following phases: registration, group key negotiation, and fast authentication. In the first phase, OBUs register to TA with their id and password. In the second phase, the protocol performs the group establishment, key negotiation, and key distribution if no group key has been shared between OBUs and RSUs. Finally, once the group key has been distributed, OBUs and RSUs can authenticate quickly.

RESULTS

Some authors have presented solutions for privacy-preserving, protection of integrity in transactions, prevention of continuous authentication, reduction of the high dependence on certifications authorities, prevention of exposure of secret keys, and regular updating of secret keys. Others have proposed solutions for reducing revoked pseudonymous lists, reducing and eliminating malicious vehicles, and improving data processing. And the rest have presented solutions for improving network scalability and time delay, reducing computation/storage/communication overhead, saving computational costs, and mitigating cybersecurity threats. Also, the solutions present the type of cryptography on which they are based and the technology they rely on to overcome certain limitations. The first group includes ECC, public-key cryptography, symmetric-key cryptography, digital signatures, and hash functions. Meanwhile, the second one includes Blockchain, Fog/Edge/Cloud computing, SDN, and NFV.

Concerning the attacks in the V2I communications, the solutions protect against replay, message forgery, impersonation, eavesdropping, DDoS, modification, Sybil, MitM, and spoofing attacks.

Based on the results, most of them have focused on preserving privacy and reducing the computational workload. Also, more than half of the solutions use any cryptography primitive, and a little less than half use any emerging technology. And finally, most of them are focused on protecting against replay and message forgery attacks.

CONCLUSION

This study provides insight into security in V2I communications. We observed that there is a slight trend toward using Elliptic Curve Cryptography instead of traditional cryptography. According to our work, around one of every three proposals use ECC on their solutions. This trend might suggest that more and more authors are betting on ECC. And although ECC is gaining popularity, it is far from being the dominant choice in cryptography.

Additionally, we observed that one part of the proposals has focused on giving a solution for privacy-preserving, protection of integrity in transactions, reduction of computation, storage, communication overhead, and saving computational costs. And the other part has focused on improving the scalability in networks and reducing network time delay.

The use of emerging technologies in security has suffered a rapid expansion. Many authors have used this type of technology to solve certain obstacles or limitations of their proposals. For instance, including Fog/Edge/Cloud computing technologies has significantly reduced computation overhead and saved computational costs. Also, this trend is evident because one of every two proposals presented in our study uses any emerging technology in their solutions. In that way, researchers must address their future work toward using emerging technologies in security in V2I communications.

REFERENCES

Abassi, R. (2019). VANET security and forensics: Challenges and opportunities. *Wiley Interdisciplinary Reviews: Forensic Science, 1*, e1324.

Ali, I., Gervais, M., Ahene, E., & Li, F. (2019). A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *Journal of Systems Architecture, 99*, 101636.

Al-Otaibi, B., Al-Nabhan, N., & Tian, Y. (2019). Privacy-Preserving Vehicular Rogue Node Detection Scheme for Fog Computing. *Sensors, 19*, 965.

Al-Shareeda, M. A., Anbar, M., Alazzawi, M. A., & Manickam, S. (2020). LSW-BVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. *IEEE Access, 8*, 170507–170518.

Ayoub, T., & Mazri, T. (2018). Security challenges in V2I architectures and proposed solutions. *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, (pp. 594–599).

Boneh, D., Goh, E.-J., & Nissim, K. (2005). Evaluating 2-DNF formulas on ciphertexts. *Theory of cryptography conference*, (pp. 325–341).

Boukerche, A., & Robson, E. (2018). Vehicular cloud computing: Architectures, applications, and mobility. *Computer networks, 135*, 171–189.

Chen, S., Hu, J., Shi, Y., Peng, Y., Fang, J., Zhao, R., & Zhao, L. (2017). Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. *IEEE Communications Standards Magazine, 1*, 70–76.

Elsadig, M. A., & Fadlalla, Y. A. (2016). VANETs security issues and challenges: A survey. *Indian Journal of Science and Technology, 9*, 1–8.

Gartner. (n.d.). Connected Cars Will Form a Major Element of the Internet of Things. *Connected Cars Will Form a Major Element of the Internet of Things.*

Gupta, M., Benson, J., Patwa, F., & Sandhu, R. (2020). Secure V2V and V2I communication in intelligent transportation using cloudlets. *IEEE Transactions on Services Computing.*

Hamdi, M. M., Audah, L., Abood, M. S., Rashid, S. A., Mustafa, A. S., Mahdi, H., & Al-Hiti, A. S. (2021). A review on various security attacks in vehicular ad hoc networks. *Bulletin of Electrical Engineering and Informatics, 10*, 2627–2635.

Islam, M., Chowdhury, M., Li, H., & Hu, H. (2018). Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention. *Transportation research record, 2672*, 66–78.

Kaur, R., Singh, T. P., & Khajuria, V. (2018). Security issues in vehicular ad-hoc network (VANET). *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, (pp. 884–889).

Kumar, A., Bansal, M., & others. (2017). A review on VANET security attacks and their countermeasure. *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, (pp. 580–585).

Liu, Y., Guo, W., Zhong, Q., & Yao, G. (2017). LVAP: Lightweight V2I authentication protocol using group communication in VANET s. *International Journal of Communication Systems, 30*, e3317.

Lv, S., & Liu, Y. (2021). PLVA: privacy-preserving and lightweight V2I authentication protocol. *IEEE Transactions on Intelligent Transportation Systems.*

Malik, A., & Pandey, B. (2018). CIAS: A Comprehensive Identity Authentication Scheme for Providing Security in VANET. *International Journal of Information Security and Privacy (IJISP), 12*, 29–41.

Manvi, S. S., & Tangade, S. (2017). A survey on authentication schemes in VANETs for secured communication. *Vehicular Communications, 9*, 19–30.

Palaniswamy, B., Camtepe, S., Foo, E., Simpson, L., Baee, M. A., & Pieprzyk, J. (2020). Continuous authentication for VANET. *Vehicular Communications*, 100255.

Park, Y., Sur, C., & Rhee, K.-H. (2016). Pseudonymous authentication for secure V2I services in cloud-based vehicular networks. *Journal of Ambient Intelligence and Humanized Computing, 7*, 661–671.

Son, S., Lee, J., Park, Y., Park, Y., & Das, A. K. (2022). Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET. *IEEE Transactions on Network Science and Engineering.*

Wang, C., Shen, J., Lai, J.-F., & Liu, J. (2020). B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs. *IEEE Transactions on Emerging Topics in Computing*.

Wei, L., Cui, J., Zhong, H., Xu, Y., & Liu, L. (2021). Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs. *IEEE Transactions on Mobile Computing*.

Zheng, D., Jing, C., Guo, R., Gao, S., & Wang, L. (2019). A traceable blockchain-based access authentication system with privacy preservation in VANETs. *IEEE Access, 7*, 117716–117726.

Zhong, H., Han, S., Cui, J., Zhang, J., & Xu, Y. (2019). Privacy-preserving authentication scheme with full aggregation in VANET. *Information Sciences, 476*, 211–221.

Zhou, F., Li, Y., & Ding, Y. (2019). Practical V2I Secure Communication Schemes for Heterogeneous VANETs. *Applied Sciences, 9*, 3131.

Zhou, Y., Liu, S., Xiao, M., Deng, S., & Wang, X. (2018). An efficient V2I authentication scheme for VANETs. *Mobile Information Systems, 2018*.