Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 5): pp. 4499-4504
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.493

A Review On Cyber Security Challenges And Resolutions For Intelligent Transportation System

Dr D.vijaya Lakshmi, Professor, HoD, IT Dept, MGIT, India, vijayadoddapaneni@yahoo.com
CH. Lakshmi kumara, Asst prof, Dept of IT, MGIT, India, chlakshmikumari_it@mgit.ac.in

ABSTRACT: In current years, automobiles became able to establish connections with other vehicles and substructure units that are located in the roadside. In the near future, the vehicular network will be extended to include the communication between vehicles and any smart devices in the roadside which is called Vehicle-toEverything (V2X) communication. The vehicular network causes many challenges due to varied nodes, various speeds and intermittent connection, where traditional security methods are not always efficacious. As a result, an extensive variety of research works has been done on optimizing security solutions whilst considering network necessities. In this paper, we present a comprehensive survey and taxonomy of the existing security solutions for V2X communication technology. Then, we provide discussions and comparisons with regard to some pertinent criteria. Also, we present a threat analysis for V2X enabling technologies. Finally, we point out the research challenges and some future directions.

Keywords: V2X communications ,LTE ,Cyber security ,Vehicular network

I. INTRODUCTION

Because of huge spread of Internet, another thought has arisen which changes inflexible articles over to brilliant items and associates them together, known as Internet of Things (IoT). This is accomplished by installing additional equipment, for example, sensors and correspondence interface inside every gadget and consolidating them with a product framework. Subsequently, the gadgets can detect the general climate and offer data utilizing remote interchanges. IoT has been extensively applied in different spaces, for example, medical services, keen urban communities and industry. Without a doubt, individuals spend the most occasions in homes, workplaces and transportation. As indicated by the U.S. Branch of Transportation and Safety Administration, individuals go through 500 million hours out of every week in the vehicle. Subsequently, in light of Alcatel–Lucent's examination which was refined in 2009, they found that more than half of members loved associated vehicles and 22% will pay expenses for correspondence administrations [10]. Subsequently, the need has been expanded for joining transportation framework under the umbrella of IoT. At first, transportation framework was changed into digital actual framework by implanting programming into vehicles. Henceforth, vehicles can shape aorganize and speak with any shrewd gadget as a piece of IoT. (Table 1) With the reconciliation of IoT advancements, vehicular organizations got helpless against different sorts of digital assaults: interior or outside assaults. Inward assaults are started by the completely approved hub which can sidestep the validation model, while outside assaults are dispatched by an unapproved hub. In the last case, secure approval model can limit the impact of these assaults. Numerous security arrangements were concentrated to ensure the vehicular organizations against different kinds of digital assaults. In this overview, we intend to give a profound examination around there and study the security answers for a wide range of vehicular correspondences. We accept that this review will manage future exploration for tending to difficulties of things to come vehicular organization.

1.1. Relations to existing surveys Despite the fact that there are an enormous number of distributions with respect to the security viewpoints in vehicular organizations, there is so far no exhaustive overview on that for Vehicle-to-Everything (V2X) correspondences. Vehicular specially appointed organization is one kind of vehicular organizations. There exist reviews zeroing in on broad construction of vehicular specially appointed organization: Al-Sultan et al. [9] gave a review on vehicular impromptu organization structure, empowering advancements, applications, and exploration challenges. Karagiannis et al. [47] proposedthe fundamental qualities and necessities of vehicular specially appointed organization, and the normalization endeavors in smart transportation frameworks. There are a few reviews on broad security challenges in vehicular specially appointed organizations as it were. For example, Al-Kahtani [7] distributed a study on the potential digital assaults on vehicular adhoc networks and the proposed security strategies to prepare for them. Engoulou et al. [26] gave security necessities and dangers in

vehicular impromptu organizations. Likewise, they talked about the assaults attributes and security arrangements. Also, Fonseca and Festag [29]evaluated the current security arrangements and depicted them on a similar level. Mishra et al. [63] introduced an overall survey of some security research in vehicular impromptu organization. Then again, there exist a few reviews on a particular security system that can be utilized in vehicular organizations. Mejri et al. [62] characterized the security arrangements in vehicular specially appointed organizations dependent on cryptographic plans and contrasted them with assess their presentation. While, Zhang [90] investigated existing trust-based arrangements in multi-specialist frameworks, portable impromptu organizations and vehicular impromptu organizations. Kerrache et al. [48] investigated the fundamental existing trust-based models and contemplated when trust-based arrangement is more appropriate than cryptography, and the inverse. In this study, we lead a top to 1. The planned taxonomy classify the security solutions of vehicular networks to study the challenges of designing security model for the V2X network which is a novel approach to the subject. 2. Threats analysis for V2X enabling technologies is conducted. Based on our knowledge, this is the first such analysis for threats in IEEE802.11p and LTE-V2X. 3. We evaluate the effectiveness of security solutions on the considered attack, message type, latency limit and model structure. The paper is organized as follow: in Section 2 we present some necessary background information. In Section 3 we mentionthe security requirements and threats analysis for V2X enabling technologies. Taxonomy of security methods for V2X technology is presented in Section 4. In Section 5, we classify and examine the presented methods. Some challenges and research direction are given in Section 6. Finally, Section 7 concludes this survey.

II. VEHICLE-TO-EVERYTHING(V2X) COMMUNICATION TECHNOLOGY

V2X technology refers to intelligent transportation system where all road entities including vehicles, pedestrians, cycles, motorcycles and infrastructure units are interconnected with each other. This connectivity will produce more accurate information about the traffic situation across the entire network. Thus, it will help in improving traffic flows and reduce accidents. In 2015, Siemens implemented the first fully dynamic system on Germany's A9 highway. The result showed 35% fewer accidents and reduction of people injured at roads with 31% [75

2.1. Architecture Astute transportation framework applies information preparing, correspondence, and sensor advances to vehicles, foundation units and side of the road clients to build security and proficiency of the transportation framework. The heterogeneous organization comprises of two principle sub-networks [35] as demonstrated in Fig. 1: • Intra-vehicle network contains an assortment of sensors which are situated in the vehicle. The associations among sensors are crossed over through Ethernet, ZigBee or WiFi associations. • Inter-vehicle network covers the correspondence between the vehicle and encompassing gadgets. It involves four elements as follows: • On-board unit is the primary element in canny transportation framework. Every vehicle is furnished with on-board unit to have the option to handle the gathered information and connect with encompassing elements. • Roadside clients, for example, passerby, motorcyclists, bikers and roller skates. • Road Side Unit (RSU) is the transportation foundation unit which exist in the side of the road. it has data about localtopology which helps with offering a few types of assistance to the street elements. • Central/Cloud worker has a focal control on all street substances, traffic and streets.

2.2. Communications V2X supports a combined connectivity raised area for the connected entities. Also, it allows road entity to transmit information such as their current speed, position, and direction to their fixed and moving adjacent entities. Then, they use this in sequence to make intelligent decision. The announcement type depends on the entities that establish the link. It supports five types of communications [1]: • Vehicle-to-Sensors (V2S) represents the communication between sensors in intra-vehicle sub-network; • Vehicle-to-Vehicle (V2V) covers the communication between vehicles using V2V application; • Vehicle-to-Pedestrian (V2P) provides the connection between the vehicle and roadside users using V2V application; • Vehicle-to-Grid (V2G) supports the communication between vehicles and the electric grid to charge Electric Vehicles. • Vehicle-to-Infrastructure (V2I) represents the communication between road entities and infrastructure units.

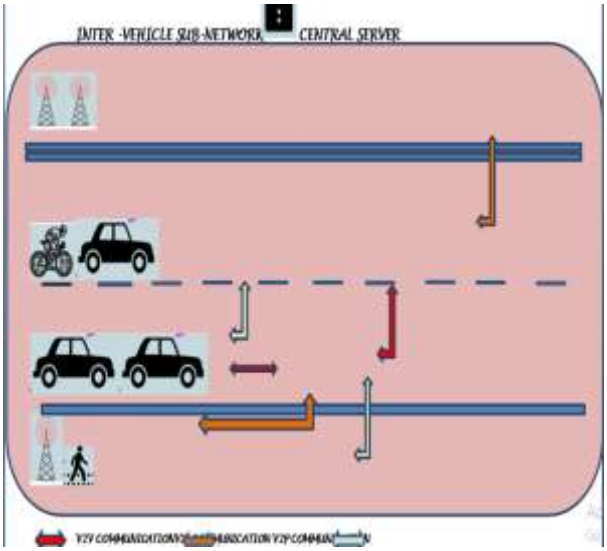


Fig. 1. General Structure of intelligent transportation system.

In one vehicular network, all road entities are theoretical to generate and exchange messages. The messages can be used to support variety of applications, e.g., applications related to safety, traffic and infotainment. The messages are categorized into four types [6]: • Periodic message (beacon): Road entity periodically broadcasts a status message, which contains information such as speed, location and direction, to the neighboring entities. It generated at regular intervals between 100ms to 1s. As a result, each entity can perceive the local topology. Also, they can predict and anticipate dangerous situations or traffic congestion. This type of messages is not time critical (300ms). • Local event triggered message: Road entity sends the message when a local event is detected such as the critical warning or intersection assist. It is sent locally to the neighboring entities using V2V/V2P links where it contains useful information for neighborhood area only. In addition, it is a time critical which requires to be delivered with a low latency around 100ms. • Global event triggered message: Road entity sends the message when a global event is detected such as road construction and road congestion. This message needs to be propagated over a wider area. As a result, road entities use V2I communication link to transmit the message. • Emergency vehicle message: It is used to support a smooth movement for emergency vehicles. It is sent by emergency vehicles to the surrounding vehicles using V2V/V2P links to clear the road

2.3. Applications

As a result of the technological improvements in the areas of sensing and wireless networking, intelligent transportation system permits for the existing of various applications that are related to safety, traffic, and infotainment [35].

• Safety-related applications use wireless communications between neighbouring entities to decrease accidents and protect the commuters from dangers. Each road entity periodically sends safety communication to its neighbours to report its current position. Furthermore, they may also need to broadcastcaution messages when local or global event is detected.

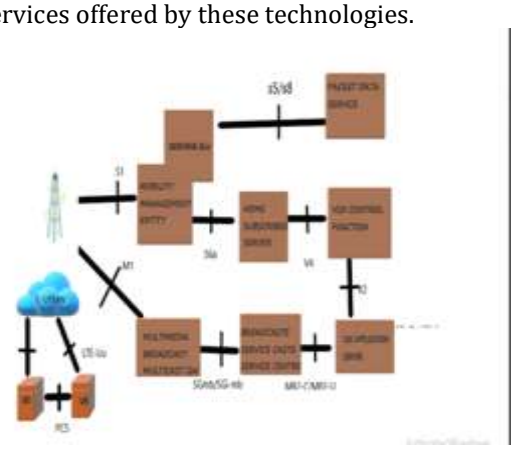
• Traffic-related applications are deployed to manage the traffic powerfully and ensure smoothly traffic flow. They are responsible for collecting the traffic information and transmitting them wirelessly to a remote server for analysis. After that, the analysis results are sent to vehicles for future usage.

• Infotainment-related applications aim at improving the driving experience by supporting various services such as Internet access, online gaming, video streaming, weather information.

III. SECURITY FOR V2X ENABLING TECHNOLOGY

Supporting safety-related applications is the core of vehicle-to-vehicle message. Since ten years ago, V2X technology has been enabled by IEEE802.11p, which has been harmonized, implemented and examined. One of the most critical challenges to make V2X technology feasible is how to ensure interoperability among varied devices. As a result, the 3rd Generation Partnership Project (3GPP) has worked on

standardization for LTE procedure to fit the needs and services of the V2X transportation. 3GPP has concentrated on following different types of transportation using one standard. The first release (Release 8) was in 2008. The standardization of LTE Advanced Pro-(Release 14) finalized at the beginning of 2017 [1]. The safety of commuters relies on the performance of these technologies. Consequently, it is important to analyse the security services offered by these technologies.



3.1. IEEE 802.11p

3.1.1. Overview It is an improved version of the ad-hoc mode in IEEE802.11a. It was implemented for supporting the message between mobile nodes with the presence of obstacles, dynamic topology and intermittent connection. The main purpose of IEEE802.11p is to support non-line of sight [28]. It was planned for following intelligent transportation system applications in vehicular adhoc networks. It provides ad-hoc announcement between vehicles and RSUs. It gives vehicles the ability to share information with their neighbouring vehicles using V2V and V2I only. IEEE 802.11p can be easily deploywith minimum cost, however, it lacks of scalability, unlimited delays, and Quality of Service (QoS). Furthermore, it can only offer intermittent V2I connectivity because of the short radio range [19].

3.1.2. Security measures

IEEE P1609.2 is based on cryptography principles such as elliptic curve cryptography, wireless access in vehicular environment certificate formats, and cross encryption methods [43]. Broadcast communicationtypically are not directed to particular destination and they related to safety-related applications. Also, they contain the timestamp which is obtained from the interior clock for harmonization. However, these messages are only signed with the sender's certificate. Elliptic Curve Digital Signature Algorithm is the signature algorithm in the standard [53]. business Messages are generally unicast messages and they may be used to access location based services and personal data. as a result, to protect the data, these messages are encrypted with a symmetric encryption algorithm. To ensure more safety, the algorithm uses random key which is encrypted using elliptic curve integrated encryption scheme [53].

3.2. LTE-V2X

3.2.1. summary It has the potential to deal with the low-latency and high reliability V2X use cases. LTE-V2X is mostly composed of six main mechanism [1] as shown in Fig. 2: Fig. 3. Communication links in LTE-V2X.

• User Equipment (UE) is the device that is used directly by an end-user to communicate with eNodeB or other UEs.

• Evolved Node B (eNB) is the wireless interface for LTE network which allows for sending and receiving radio transmissions to/from all UEs in one or more cells.

• V2X Application Server is responsible for distribution of V2X messages to different target areas.

• V2X Control Function is responsible for authorization and revocation of V2X services. It provides various services after successful mutual authentication and security key generation.

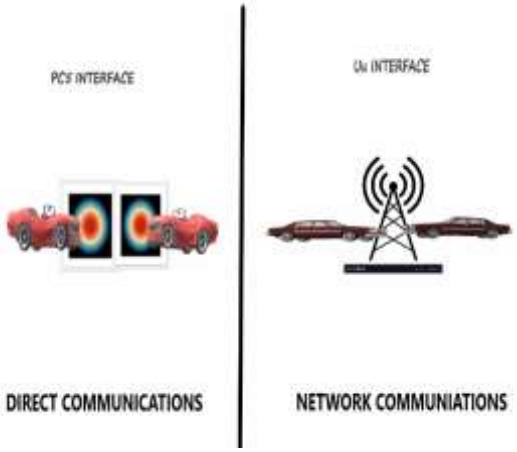
• Multimedia Broadcast Multicast Service supports efficient delivery for multicast services over areas typically spanning multiple cells.

• Single-cell Point-to-Multipoint provides the delivery of multicast services over a single cell. In LTE-V2X, the messages are sent using two types of links, as shown in Fig. 3:

• Cellular-based announcement covers the two way communication between UE and eNB over LTE air interface [11]. The communication going from UE to eNB is called uplink and when it is going from eNB to a UE it is called downlink. Cellularbased communication covers wide area with high capacity. It is used by V2X application server to broadcast messages to vehicles and beyond, or send them to the server via a unicast connection. In addition to one-to-one communications be-tween eNB and UE, eNB supports one-to-many communications via downlink. eNB uses single-cell point-to-multipoint service for the

transmissions over a single cell and multimedia broadcast multicast service for communications over multiple cells.

• Device-to-Device communication (D2D) enables the direct connection between UEs without traversing eNB and it is called side-link. It supports multi-hop communications between network entities to enhance the end-to end connectivity. Also, it provides a short-range communication and low latency for safety messages. It allows for UE to transmit data directly to other UEs over the side-link even if they reside out-of-network coverage. Every D2D pair can communicate via Inband or Outband modes [11]. In band mode uses the cellular spectrum for both D2D and cellular communications. Underlay communication allows for both of them sharing and reusing the same radio resources to improve the spectrum efficiency. The main drawback is the high possibility of collision between D2D links and cellular links. In contrast, overlay communication allocates dedicated cellular resources for D2D connections between the transmitter and the receiver. To minimize the interference between D2D and cellular links, out band mode uses unlicensed spectrum such as 2.4 GHz manufacturing, scientific and check-up radio band. However, it is necessary to have an extra border that implements Wi-Fi Direct or Bluetooth.



IV. CONCLUSION

The rapid evolution of the transportation sector has caused security challenges which made the vehicular network vulnerable to various cyber-attacks that hinder the secure V2X communication. In addition, we should take into account the features of the V2X network while designing the security model. In this survey paper, we first clarified the key features and architecture of the V2X network. Also, we proposed the threats analysis for V2X enabling technologies. Then, we classified the current security solutions in vehicular networks based on the security method. Also, we presented the comparison and discussion of various security methods. Finally, we mentioned the main challenges and future research directions for novel contributions to this research area. As a conclusion, combining cryptography and trust strategies will protect the network from internal and external attacks and thus guarantee high security level.

REFERENCES

[1]3GPP,UniversalMobile Telecommunications System (UMTS); LTE; Architecture enhancement for V2X Services (3GPP TS 23.285 version 14.2.0 Release 14), Technical Report, ETSI, 2017.

[2] 5G-Americas, V2X Cellular Solutions, Technical Report, 2016.

[3] K.C. Abdelaziz, N. Lagraa, A. Lakas, Trust model with delayed verification for message relay in VANETs, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International, IEEE, 2014, pp. 700–705.

[4] A.M. Abdelgader, F. Shu, Exploiting the physical layer security for providing a simple user privacy security system for vehicular networks, in: Communication, Control, Computing and Electronics Engineering (ICCCCEE), 2017 International Conference on, IEEE, 2017, pp. 1–6.

[5] A. Ahmed, K.A. Bakar, M.I. Channa, K. Haseeb, A.W. Khan, TERP: a trust and energy aware routing protocol for wireless sensor network, IEEE Sens. J. 15 (12) (2015) 6962–6972. [6] K.J. Ahmed, M.J. Lee, Secure, LTE-based V2X service, IEEE Internet Things J. (2017).

[7] M.S. Al-Kahtani, Survey on security attacks in vehicular ad hoc networks (VANETs), in: Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, IEEE, 2012, pp. 1–9.

[8] M. Al Mutaz, L. Malott, S. Chellappan, Leveraging platoon dispersion for sybil detection in vehicular networks, in: Proceedings of the Eleventh Annual International Conference on Privacy, Security and Trust (PST), IEEE, 2013, pp. 340–347.
[9] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, J. Network Comput. Appl. 37 (2014) 380–392.
[10] G. Araniti, C. Campolo, M. Condoluci, A. Iera, A. Molinaro, Lte for vehicular networking: a survey, IEEE Commun. Mag. 51 (5) (2013) 148–157.
[11] A. Asadi, Q. Wang, V. Mancuso, A survey on device-to-device communication in cellular networks, IEEE Commun. Surv. Tut. 16 (4) (2014) 1801–1819.
[12] R.S. Bali, N. Kumar, Secure clustering for efficient data dissemination in vehicular cyber–physical systems, Future Gener. Comput. Syst. 56 (2016) 476–492.
[13] S.K. Bhoi, P.M. Khilar, SIR: a secure and intelligent routing protocol for vehicular ad-hoc network, IET Netw. 4 (3) (2014) 185–194.
[14] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2004, pp. 506–522.
[15] C. Chen, J. Zhang, R. Cohen, P.-H. Ho, A trust modeling framework for message propagation and evaluation in VANETs, in: Information Technology Convergence and Services (ITCS), 2010 2nd InternationalConferenceon,IEEE, 2010, pp. 1–8.