DOI: http://dx.doi.org/10.26483/ijarcs.v15i6.7159

ISSN No. 0976-5697

Volume 15, No. 6, November-December 2024

nternational Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

STUDY OF VANET COMMUNICATION ARCHITECTURE AND CHALLENGES FOR SECURITY SOLUTIONS

Sonia
Research Scholar, NIILM University,
Kaithal, India

Pawan Kumar
Assoc. Professor, NIILM University,
Kaithal India

Abstract: VANETs are useful for V2V (vehicle-to-vehicle) communications in such a special network. Vehicles can also communicate with roadside infrastructure (V2I). These are two important, logical, and useful features of VANET. V2I enables the mobile node to connect to the Internet and enables global communication on the go. The detailed V2V function allows the exchange of data, for example, accidents and environmental conditions [5]. The idea of utilizing radio communications in vehicles to enhance safety has been around for a long time, even before the appearance of digital communications. In recent years, vehicle safety has been focused on communication between vehicles.

Keywords: VANET, Digital Communication.

1.1Introduction to VANET:

In the mid-1980s, CAN (Controller Area Network), the earliestcar controller network, was created by Bosch and is presently utilized in few other automation applications. In 2000, CAN, as an ISO 11898 standard, was the most utilized automotive network with over 100 million CAN nodes traded. CAN be a serial data bus for applications working at data rates up to 01 Mbps, with error detection and other features. A vehicle may comprise of a few unique CANs working at various transmission rates [7].

In 1984, the Radio Data System Communication Protocol (RDS), which included limited quantities of digital information in radio frequency-modulated (FM) transmissions to transmit more audio signals over radio waves, turned into the main digital infrastructure for a vehicle (I2V), and a few years later it was announced in the United States as a Radio Data System. The “Radio Data System (RDS)” turned into the European standard in 1991. The data rate in both RDS and RBDS was 1187.5 bits per second on 57 kHz subcarrier. The data was sent with error adjustment, by including numerous elements of the RDS system, given that it was a unidirectional system [6].

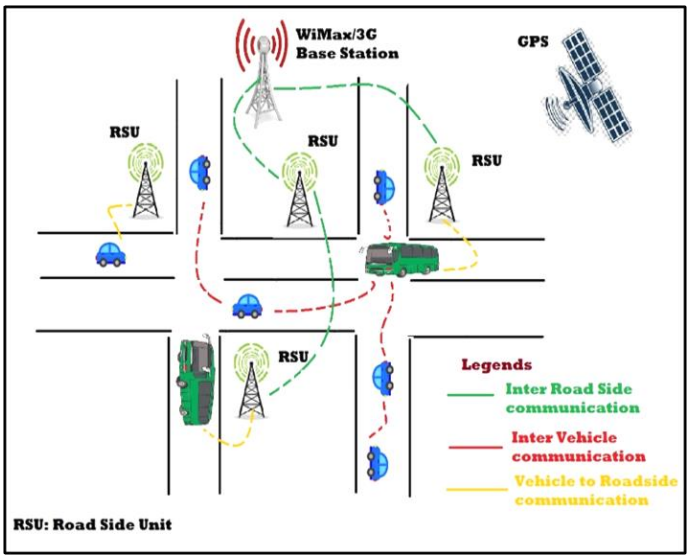

Figure 1.1: Vehicular Ad hoc Networks

The first two-way communication systems developed during the 1980s using tolling frameworks in which RFID tags were entered into vehicles (“mainly up to 2.45 GHz, and then transmitted up to 5.8 GHz in Europe and the USA at 915 MHz”). For the first time, it was recommended that the dedicated 5.8 GHz short-range communication system (DSRC), created by Philips in the mid-1990s as a kind of the 2.45 GHz system, should

turn into the "Intelligent Vehicle and Highway Systems (IVHS)" for communication. Since this on-board DSRC system was capable of performing various kinds of exchanges, in the inappropriate world of telephony and the Internet of the 90s, it was proposed to become a recognizable means of providing IVHS services [6].

1.2 VANETs Architecture

In VANET, the RSUs are placed along the roadside to provide infrastructure-based services to the vehicles. The vehicular communication aims to save the lives of drivers by broadcasting real-time safety information such as vehicle collisions, accidents and road conditions (Javier Ibanez-Guzman et al., 2010). Thus, the vehicular communication provides safe & comfortable driving environment for the drivers [3]. Figure 1.1 depicts architecture of communication in VANET: -

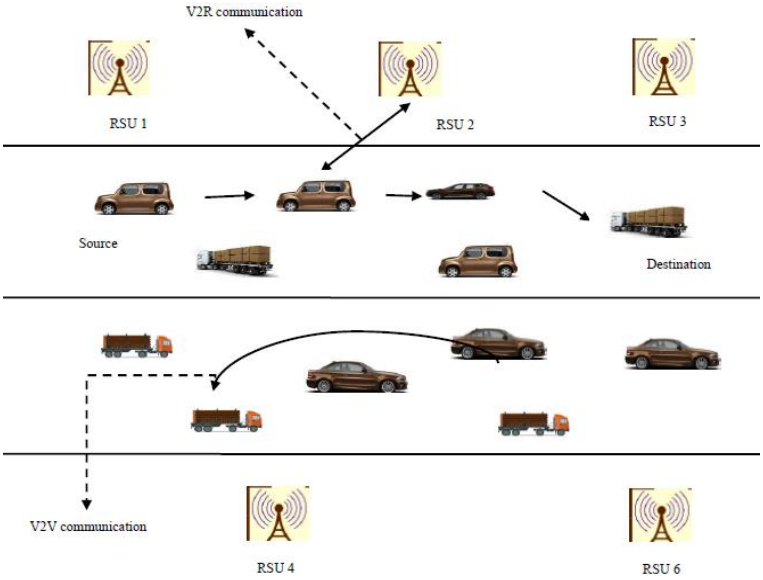

Figure 1.2 Architecture of VANET Communication

There are mainly two types of communication scenarios in VANET such as V2V and V2R:-

i) **Vehicle-to-Vehicle (V2V):** It is referred as intra vehicle communications, in which the vehicles can transmit the safety-related information such as traffic conditions and accidents on roads to others.

ii) **Vehicle-to-RSU (V2R):** In V2R communication, the vehicles can communicate with RSUs and obtain roadside information such as parking availability, hotels, and coffee shop. The V2R communication is also referred as inter-vehicle communication.

1.3 Challenges in VANET Security Solutions

The different applications of VANET have diverse security requirements The defense schemes must ensure that the packet originator is a trusted vehicle. Due to the features of VANET, exceptionally high speed of vehicles and frequent topology changes, the VANET security is quite difficult. An effective defense system is needed to establish the liability of drivers while preserving their location and identity privacy. The VANET security system faces the following challenges [4]:-

i. **Mobility:** The node mobility is a significant factor for vehicular networks. The mobility of vehicles is measured in miles, not meters per hour. High-speed vehicles cause frequent link disconnections and makes the communication highly unreliable. The temporary communication links in a VANET degrades the efficiency of security systems.

ii. **Privacy and Security:** The characteristics of VANET such as high mobility, high reliability, and unreliable communication medium increase the security and privacy concerns while transmitting safety-related messages. These safety messages comprise verifiable identity, current location, speed and acceleration of a vehicle. The safety messages assist drivers to take sensible driving decisions based on traffic jam and road conditions. Although these safety messages prevent accidents, they are vulnerable to track the location of a victim vehicle by an unauthorized vehicle, as the nature of the wireless medium in VANET allows anybody to receive the broadcast messages. To prevent the vehicle privacy and security attacks, each vehicle binds with secret keys. For instance, the malicious nodes claim to be hundreds of vehicles to create the illusion of a congested road. According to the congestion control mechanism, the legitimate vehicle decides another longest route for traveling. Authentication is a keys security requirement in VANETs to validate the packet sender and to prevent attacks on VANETs.

iii) **Availability:** The availability of network is vital for delay tolerant real-time applications. However, meeting the requirements of real-time applications is highly vulnerable to Denial of Service (DoS) attacks. In the deceleration application, the time to live of data packets is a fraction of a second and even less than the second the packets are considered as meaningless. The unreliable wireless communication between the vehicles further aggravates the routing problem during delay sensitive packet transmission. Most of the VANET routing protocols provide an acceptable latency and high data rate, but the reliability and security are still missing in VANETs communications.

iv) **Low Fault Tolerance:** The VANET is highly sensitive to the computational error. Most of the secure routing protocols exploit probabilistic schemes for VANETs' safety-related applications. However, even a small probability of error tends to multiply accidents on the road.

v) **Key Distribution:** The key distribution is the main component in the design of secure routing protocol. The conventional key distribution schemes face different challenges. There is a lack of coordination and interoperability between the key distributors and vehicles. The potential approach for secure key distribution is to empower the Motor Vehicles licensing authority to take the role of a certificate authority. However, this approach also has the number of limitations regarding the vehicle privacy. Thus, there is a need to design a secure and privacy-preserving key distribution algorithm for VANETs.

vi) **Cooperation:** The VANET applications require cooperation among the vehicles during packet routing. Principally, the VANETs comprises a huge number of high-speed vehicles. In real time applications of VANET, the efficacy of cooperation and information sharing among vehicles relies on the relative speed of vehicles. In safety applications, it is essential that the vehicles must identify the accidents and inform other vehicles to make the driving comfortable.

1.4 Attacks and Issues in VANET Communication

The secure wireless communication is a significant challenge in VANETs, having a great impact on the applications of vehicular networks. Indeed, communication security and location privacy are major concerns in the acceptance of VANET services. The effectiveness & reliability of safety message dissemination in VANET raise concerns about location privacy and data authenticity. In location privacy, there are different goals at the sender & receiver of messages. The receiver goal is to ensure the strong message authentication, whereas, at the sender side, the goal is to provide the strong location privacy. VANETs are also at risk for a wide range of attacks. It poses many drifts on technology, rules and refuge which need to undergo further need for research. VANETs alters each share of vehicles into a remote switch or node, letting from 100 to 300 meters from one another to interface and, thusly making network with a wide range.

i) Sybil Attack: - Sybil attack is a significant concern in VANETs in which a malicious vehicle pretends as multiple identities that overwhelmingly influence the driving decisions (Douceur and John., 2002). The malicious node impersonates other vehicles or road-side infrastructure to trigger safety hazards. A malicious vehicle misrepresents the information in warning messages and broadcasts the false data to gain an advantage. For instance, a malicious vehicle reports that the road is jammed with traffic, thereby encouraging others to avoid the particular road and enjoying a less congested journey on the road. Due to the impersonation, the detection of sybil attack is quite complex in VANETs. Therefore, it is crucial to develop security mechanisms to detect the sybil attack [2].

ii) Eavesdropping during Broadcasting scheme: - The broadcasting scheme in intra vehicle communication is used for safety applications. The safety messages assist drivers to take sensible driving decisions based on traffic jam and road conditions. Although these safety messages help in preventing accidents, they are vulnerable to track the location of a victim vehicle by an unauthorized vehicle as the nature of communication in VANETs is wireless which allows anybody to access the broadcasted messages. An attacker easily eavesdrops the broadcasted messages, and it collects the locations that are visited by a victim vehicle over particular time. Thus, the malicious vehicle performs crime and automobile thefts. Hence, it is crucial to maintain the location information of vehicles during the journey secretly [6].

iii) Attack on cryptographic keys: - The cryptographic techniques provide cryptographic keys to ensure authenticity in vehicular communication. The vehicles encrypt & decrypt the broadcast messages using the cryptographic key pair. However, an attacker tracks the cryptographic keys by overhearing the communication of its neighboring vehicles and launches different types of attack into the network [2].

REFERENCES

[1] F. Akyildiz, W. Su, Y. S. Subramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, August (2002).

[2] Marvy B. Mansour1 , Cherif Salama2 , Hoda K. Mohamed3 and Sherif A. Hammad4 International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.2, March (2018)

[3] Mohammad Jalil Piran , G. Rama Murthy , G. Praveen Babu "Adhoc and sensor networks; principles and challenges" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.2, June(2011) . Security Comm. Networks 2011; 4:1137–1152 Published online 15 July 2010 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.239

[4] Muhammad Sameer Sheikh 1,2, Jun Liang 2,* and Wensong Wang " A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)" "Sensors 2019, 19, 3589; doi:10.3390/s19163589 Aug (2019).

[5] Congcong Li 1,*, Xi Zhang 1 , Haiping Wang 2 and Dongfeng Li "An Enhanced Secure Identity-Based Certificateless Public Key Authentication Scheme for Vehicular Sensor Networks" Sensors 2018, 18, 194; doi:10.3390/s18010194 January (2018)

[6] Harry Gao, Seth Utecht, Gregory Patrick, George Hsieh, Fengyuan Xu, Haodong Wang, Qun Li "High Speed Data Routing in Vehicular Sensor Networks" "Journal of communications, vol. 5, no. 3, march (2010)

[7] Jaehoon Paul Jeong , Tae Tom Oh , Sangheon Pack Alexandre Petrescu " Protocols and applications in vehicular sensor networks for driving safety, driving efficiency, and data services" "International Journal of Distributed Sensor Networks, Vol. 13(2) (2017)

[8] Lin, X.; Lu, R.; Zhang, C.; Zhu, H.; Ho, P.; Shen, X. Security in vehicular Ad-hoc networks. IEEE Commun. Mag., 46, 88–95 (2008).

[9]. Riley, M.; Akkaya, K.; Fong, K. A survey of authentication schemes for vehicular ad hoc networks. Secur. Commun. Netw. Volume4, Issue10 (2011)

[10]. Manvi, S.S.; Tangade, S. A Survey on Authentication Schemes in VANETs for Secured Communication. Veh. Commun. Volume 9 (2017)

[11]. Sharma, S.; Kaul, A. A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. Veh. Commun. Vol 12 (2018)

[12] Paruchuri, V.; Durresi, A. PAAVE: Protocol for anonymous authentication in vehicular networks using smart cards. December (2010);

[13]. Almeida, J.; Shintre, S.; Boban, M.; Barros, J. Probabilistic key distribution in vehicular networks with infrastructure support. In Proceedings of the Global Communications Conference, Anaheim, CA, USA, 3–7 December 2012; pp. 973–978.

[14] Zhang, C.; Lin, X.; Lu, R.; Ho, P.H. RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks. In Proceedings of the International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 1451–1457.

[15]. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K. SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad. Hoc. Netw. Volume 9 (2011)

