A comparative study of the Security Protocols in VANET

Simple Nain[1], Sandeep Tayal[2]

[1]M.tech Student, Department of ECE, Vaish college of Engineering, Rohtak
Nainsimple28@gmail.com

[2]Associate Professor, Department of ECE,Vaish College of Engg., Rohtak, Haryana-124001, India
tayalsan@gmail.com

Abstract

Vehicular Ad Hoc Networks (VANET) is a subclass of Mobile Ad Hoc networks. In VANET, Wireless device sends information to nearby vehicles, and messages can be transmitted from one vehicle to another vehicle or roadside infrastructure. So, using VANET can increase safety and traffic optimization. Similar to other technologies, in VANET there are some important and noticeable issues. One of the most important of them is Security. Since the network is open and accessible from everywhere in the VANET radio range, it is expected to be an easy target for malicious users. Therefore, the survey of the security protocols in VANET is important. The paper discusses the advantages and disadvantages of these security protocols. Finally, a comparison of the various security protocols is shown.

Keywords: *VANET, Security Protocols, MAC Protocols.*

1. Introduction

A Vehicular Ad Hoc network is a form of Mobile Ad Hoc network, to provide communication among nearby vehicles and between vehicles and nearby fixed equipment i.e. roadside equipment. The main goal of VANET is providing safety and comfort for passengers. Each vehicle equipped with VANET device will be a node in the Ad-hoc network and can receive and relay other messages through wireless network. VANET provides an intelligent way of using vehicular networking. With the sharp increase of vehicles on roads in the recent years, driving becomes more challenging and dangerous. Now days, roads are saturated, therefore, the safety distance and reasonable speeds are highly valued. The leading car manufacturer decided to jointly work with government agencies to develop solution aimed at helping drivers on the roads by anticipating hazardous events or bad traffic areas. One of the outcomes has been a novel type of wireless access called wireless access for vehicular environment (WAVE) used for vehicle to vehicle and vehicle to road side communication.

VANET integrates multiple Ad-Hoc networking technologies such as WiFi IEEE 802.11 b/g, WiMAX 802.16, Bluetooth, IRA, Zigbee for accurate, effective and simple communication between vehicles on dynamic mobility.

2. SECURITY CHALLENGES IN VANETS

Unauthorized access, while the authorities should be able to access such information to look for witnesses in case of a dispute such as a crime/car accident scene investigation. The user-related information includes the driver name, license plate, speed, position, and travelling routes.

Liability Identification: Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes or the transportation system. As part of the "conditional privacy" requirement, the authorities should be able to determine the identities of message senders in the case of a dispute.

Jamming: The jammer deliberately generates interfering transmissions that prevent legal communications within their reception range. In the VANET scenario, an attacker can relatively easily partition the network without compromising cryptographic mechanisms and with limited transmission power.

Impersonation: An attacker can electronically pretend to be as an emergency vehicle to mislead other vehicles to slow down and yield. So an impersonator can be a threat. Message fabrication, alteration, and replay can all be used towards impersonation.

Privacy Violation: The collection of vehicle-specific information from overheard vehicular communications will be easy when VANETs are deployed. Then inferences on the personal data of drivers could be made, thus violating the privacy of drivers.

Forgery: An attacker can forge and transmit false hazard warning information or other messages, which can rapidly contaminate large portions of the

VANET coverage area. The correctness and timely receipt of application data is a major vulnerability.

3. OVERVIEW OF SECURITY PROTOCOLS

In VANET, the following security protocols have been proposed:

3.1 A Security Protocol for Vehicular distributed systems

This protocol guarantees the content of messages against possible attackers. Because privacy of the passengers must be preserved in VANET, this security protocol is designed not to rely on the driver's identity. The protocol also proves the time and location when a message was sent. The security protocol considers the particular characteristics of VANETs. It ensures data integrity, reliability, non-repudiation, preserves privacy and links a message to a particular time and place the message was generated. The security protocol is implemented in VANET simulator and the evaluation result shows its capability to handle a wide range of attacks that are characteristic to such environments.

3.2 A Secure VANET MAC Protocol for DSRC applications

A secure MAC protocol for VANETs has different message priorities for different types of applications to access DSRC channels. The MAC protocol can provide secure communications while guarantee the reliability and latency requirements of safety related DSRC applications for VANETs. The secure communication protocol is designed to guarantee the freshness of the message, message authentication and integrity, message non-repudiation, and privacy and anonymity of the senders.

3.3 Cognitive security protocol for sensor based VANET using swarm intelligence

The cognitive security protocol disseminates information using distributed sensor technology while prioritizing prevention of data aging, efficient quality of service (QoS) and robustness against denial-of-service (DoS) attack. The reliability and optimality of the protocol is computed based on current mission response time and maintaining message authentication, integrity, confidentiality and non-repudiation. DoS, is an act by adversary to reduce the reliability of the application. There are two types of DoS attacks, Sybil and Collision. These two attacks leads to packet loss, localisation error and integrity of information transmitted. Due to the varied design constraints and missions in S-VANET, a nature inspired framework and optimisation technique is applied to the protocol. The process of identifying an intrusion is based on agent's performance matrices i.e., PDR energy, BER, distance, hop stored in the tubulise form. When the agent senses a sudden change in PDR from its previous tour, it flags the node and updates globally.

3.4 Real-World VANET security protocol

Real-world VANET security protocol used recordings of actual vehicle movements on various roadways. The simulation of the protocol used as input, traces of vehicles movements that have been generated by traffic simulators which are based on traffic theory models. Till now, no one has published any work based on actual large-scale recordings of vehicle movements. In order to enable analysis on this scale, a new VANET simulator is developed, which can handle many more vehicles than NS-2. To use this simulator, the researcher presented results of a cross-validation between NS-2 and their simulator, showing that both simulators produce results that are statistically the same. The evaluations are performed using real vehicle mobility, which is the first simulation using real vehicle mobility.

3.5 A secure fire truck communication protocol for VANET

A secure fire truck communication protocol is a secure emergency vehicle transmission protocol for VANET to ensure the messages will not be revealed or stolen. The protocol combines symmetric encryption and digital signature mechanism. The protocol can achieve the mutual authentication, session key security, known-key security and prevent the known attacks. This protocol works efficiently in urban environment.

Table 1 gives a Comparison of these protocols.

Protocols	Security protocol for vehicular distributed systems	A Secure VANET MAC protocol for DSRC applications	Cognitive security protocol	Real-World VANET security protocol	A Secure fire truck communication protocol
Data integrity	Yes	Yes	Yes	No	Yes
Reliability	Yes	Yes	Yes	Less reliable	Less reliable
Non-repudiation	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	Yes
Scenario	Urban	Urban	Urban	Urban	Urban
Realistic traffic flow	No	No	No	Yes	No

4. Conclusion & Future Perspectives

Message Integrity ensures that messages must be protected from any alteration and the receiver of a message must confirm the sender of the message. All the protocols discussed above provide data integrity except the real-world VANET security protocol. Message Non-Repudiation ensures that the sender of a message cannot deny having sent the message. All the security protocols discussed above ensure message non-repudiation. Entity Authentication ensures that the receiver is not only ensured that the sender generated the message, but in addition has evidence that the sender is a network node.

The future perspectives for VANET security protocols should include following:

1. A major challenge in protocol design in VANET is to improve reliability of Protocols and to reduce delivery delay time and the number of packet retransmission.

2. To design and implement the protocols for rural environments as well.

5. References

[1] Catalin Gosman, Ciprian Dobre, Valentin Cristea, "A Security Protocol for vehicular distributed systems", 12th international conference on symbolic and numeric algorithms for scientific

[2] Jason J. Haas and Yih-Chun Hu, Kenneth P.Laberteaux, "Real-World VANET Security Protocols Performance", Globecom, pp. 1-7,2009, IEEE digital library.

[3] Rajani Muraleedharan and Lisa Ann Osadciw, "Cognitive Security Protocol for Sensor Based VANET Using Swarm Intelligence", Asilmore, pp. 288-290, 2009

[4] Chin-Ling Chen, Chun-Hsin Chang, "A Secure fire truck communication protocol for VANET", Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taiwan.

[5] C.K.Toh, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*", Prentice Hall Englewood Cliff, NJ 07632, 2002.

[6] C. Perkins, "*Ad hoc Networks*", Addison-Wesley, 2012

[7] Dedicated Short Range Communications (DSRC) Home, http://www.learmstrong.com/DSRC/DSRCHomeset.htm.

[8] Elmar Schoch, Frank Kargl, Michael Weber, and Tim Leinmuller "*Communication Patterns in VANETs*", IEEE Communications Magazine, 46:119–125, Nov 2009.

[9] Ghassan Samara, Wafaa A.H. Al-Salihy, R.Sures, "*Security Issues and Challenges of* [11] Gongjun Yan, Gyanesh Choudhary, Michele C.Weigle, Stephan Olariu, "VANET' 07 Poster: Providing VANET Security through Active Position Detection", Department of Computer Science, Old Dominion University, Norfolk, USA.

[10] Shankar Yanamandram, Hamid Shahnasser, "Analysis of DSRC based MAC protocols for VANETs", International conference on ultra modern telecommunications and workshop, 2009