International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 11 November 2018

ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks

Pooja Mehra[1] and Dr. Harish Patidar[2]
Dept of CSE, Lakshmi Narain College of Technology, Indore, MP, India[1, 2]
mehra.pooja12345@gmail.com[1], harish.cs@lnctindore.com[2]

Abstract: *Vehicular ad hoc Networks (VANETs) allow vehicles to form a self- organized network. VANETs are likely to be widely deployed in the future, given the interest shown by industry in self-driving cars and satisfying their customers various interests. Problems related to Mobile ad-hoc Networks (MANETs) such as routing, security, etc. have been extensively studied. Even though VANETs are special type of MANETs, solutions proposed for MANETs cannot be directly applied to VANETs because all problems related to MANETs have been studied for small networks. Moreover, in MANETs, nodes can move randomly. On the other hand, movement of nodes in VANETs are constrained to roads and the number of nodes in VANETs is large and covers typically large area.*

Keywords: *Vehicular Ad Hoc Networks, Vehicular Communication and Security and Privacy in Vehicular Networks.*

1. INTRODUCTION

Mobile Vehicular Ad Hoc Networks (VANETs)[1] provide ubiquitous connectivity to mobile users on the road and efficient vehicle-to-vehicle communication that can help in implementing Intelligent Transportation Systems (ITS). ITS can provide support for various types of applications such as collision prevention, traffic monitoring, traffic own control, providing information about nearby services [3]. Another important application of VANETs is that since vehicles are connected to the Internet, the users could enjoy the services, the infotainment, and the entertainments, supported on the Internet while they are moving.

VANETs are special type of MANETs (Mobile Ad hoc Networks)[2]. The main difference between the two is that nodes in VANETs are vehicles on the roadway and their movement is constrained to roads whereas nodes in MANETs move randomly. One of the primary goals of VANETs is to increase road safety. In order to achieve this goal, vehicles monitor phenomena on the roads and inform other vehicles about abnormal and dangerous traffic condition such as icy roads, heavy congestion, or car accidents. Adversaries could exploit this by injecting malicious messages for their own benefit or to deliberately disrupt the users. Thus, securing VANETs from such adversaries is important.

In VANETs, each vehicle is equipped with a communication device to communicate with other vehicles and designated roadside infrastructure, called road side units, to exchange safety related information. These vehicle nodes and roadside infrastructure together form a self-organized network, called a Vehicular Ad-hoc Network. In VANETs, various type of techniques is required such as beaconing, forwarding, broadcasting, and routing to deliver messages to the destination through appropriate nodes[4]. Due to the high mobility of vehicle nodes, the network topology changes frequently. Our main aim is to address the security and routing issues in VANETs. Next, we present the necessary background, motivation for our research, and the problems addressed in this dissertation.

1.1 Background

In this section, we introduce the security architecture, trust issues, key and certificate management, and attacks in VANETs and existing solutions, which our research is based on.

1.1.1 Security Architecture

Requirements of Security Services

Security mechanisms in MANETs[5] have been extensively studied; however, they are not suitable for VANETs due to the unique characteristics of VANETs, so they can't be directly applied to VANETs[6]. Despite a broad range of challenges facing securing vehicular communication, the security issues must be addressed and solved for the successful deployment of VANETs. Since the drivers and the vehicles in VANETs rely on shared information to make decisions, they would be vulnerable to malicious and misbehaving nodes; so proper mechanisms need to be implemented for detecting and thwarting attacks from such malicious nodes. The security services of VANETs typically need to meet the following requirements.

- Integrity: The integrity service is to deal with the accuracy, consistency, and the completeness of messages during transmission. In order to prevent attackers from altering or injecting messages, integrity of messages should be ensured .Also, a reliable time source for accurate time synchronization and a reliable positioning system for precise location information could be used to protect communication against attacks such as replay-attack or position spoofing attack.
- Availability: In VANETs, time critical messages such as emergency traffic information must be handled at any given time. If one channel is not available due to failure or attack, there must be alternative means to maintain vehicular network availability all the time.
- Authentication: Every message exchanged must be authenticated to identify the sender of the message. Vehicles should react only to information or events generated by legitimate senders.
- Non-repudiation: This service is designed to identify misbehaving nodes or attackers and prevent them from denying messages transmitted by them. Any vehicle related information for communication, such as location, speed, and time, will be stored in a tamper-proof On-Board Unit. It also could be used by authorities for investigation to reproduce the scene of an accident with the same sequence and content of the messages communicated before the accident.
- Real-time constraints: Vehicles move with high velocity. In some situations like time-sensitive communication, a real-time response is essential, so time constraints should be respected.
- Privacy: All driver information such as identity, location and speed, should be protected against unauthorized observers. Also, an observer should not be able to trace the routes of the vehicles.

Network Model

Two types of communicating entities are presented in the currently explored architectures of VANETs. The first type is a vehicle node which forms the majority of all VANET nodes .The second type is the roadside base stations, usually called RSUs (Road Side Units)[7]. The radio used for communication is Dedicated Short-Range Communications (DSRC)[8], which has been allocated as a new band in 1999 by the Federal Communications Commission; the band allocated was 75MHz at 5.9GHz frequency for Intelligent Transport System (ITS) applications in North America. Also, the IEEE802.11p standard supports the communication channel and technology. Communication in VANETs could be either direct communication between vehicles or through multiple wireless link hops. Vehicles operate as both endpoints and routers. Vehicular networking will enable vehicle-to-vehicle communication, vehicle-to-RSU communication and vehicle-to-existing infrastructure networks communication.

High velocity of vehicle is a real-time constraint in VANETs. For example, if two vehicles are moving in opposite direction on highways, they would only have a very short connection time between them. Also, unlike MANETs in which nodes move randomly, vehicles move along the roads, hence their mobility is constrained .Vehicles in VANET are equipped with a wireless communication device and computation resources to perform security tasks. Also, additional devices such as a Global Positioning System (GPS)[9] and an Event Data Recorder (EDR)[10] could be present to provide the location of vehicles. Vehicles also have a tamper-proof storage for private information such as private/public keys and electronic license plate information.

Message Categories

Many applications are waiting for deployment in VANETs. These applications can be divided into two major categories, namely safety related applications and non-safety related applications.

- Safety-related applications

For example, collision avoidance warning messages, emergency brake warning messages, traffic light warning messages, or lane merging warning messages could be sent to warn drivers. Since the messages sent by this type of application help drivers make critical decisions, ensuring the security and reliability of such messages is essential.

- Traffic information messages: Messages contain information such as road condition and accidents. Messages are sent to all vehicles within specific area for safety and typically they are not time-critical messages.
- General safety-related messages: This type of messages is used for general safety applications such as cooperative driving. Due to the high mobility of vehicle nodes, message contents are time sensitive, hence they should arrive within the preset time window.
- Liability-related messages: This type of messages is used for liability-related applications, which share traffic information and drivers are responsible for the traffic information. For example, if the message originator need be traced back to investigate an accident by the law enforcement authorities, the authorities should be able to trace the message to its sender.
- Non-safety-related Application

There are non-safety related applications, such as traffic optimization, automatic payment services, location-related services, and driver infotainment services. This type of applications do not have time-critical messages, but securing messages for such services (e.g., payment services) and protecting user privacy (e.g., location service) are still very important for such applications.

2. TRUST ISSUES

Establishing trust between communicating vehicles is still one of the major challenging problems. Especially in safety applications, trust is a key element as receiving nodes make decisions with the critical information from the safety application while moving at high speed. Therefore, VANETs should ensure authenticity and trust ability of every message before using it.

In VANETs, each node needs to be equipped with a trust system that can make trust decisions. There are two approaches to establish trust. The first approach is the infrastructure-based trust establishment, which relies on trusted and global central authority. Another approach is the self-organizing trust establishment, where the system is built up and adapted dynamically for the environment [11]. The details of these approaches are discussed next.

Infrastructure-based Trust Establishment

There are many approaches for infrastructure based trust establishment. In this type of trust establishment, trust relies on a static security infrastructure and certificates are used in most cases. Here, we review some such approaches.

- Classical Certificate-based Systems: This is the traditional trust system with certificates. At the initial stage, certificates are issued by a central authority and later they are used for trust verification. One of the example is the simple Public Key Infrastructure, where trust is based on the public keys of nodes
- Kerberos: Kerberos system is designed to improve security and prevent replay attacks. In Kerberos system, a central Key Distribution Center (KDC)[12] authenticates users to issue a valid trust token. The trust token contains a session key, a validity period, and the requesting node's identity encrypted with the server's secret key.

Self-organizing Trust Establishment

VANETs require a modified form of trust establishment due to the highly dynamic nodes. Connection to the security infrastructure for verification may not be available all the time. Also, nodes may need to make a decision quickly based on unverified information, which is sent by unidentified nodes. Hence, for self-organizing trust establishment 1) no trusted third party is involved. (e.g., online infrastructure) and 2) no global knowledge is shared between the nodes.

Trust relationships in VANETs change dynamically with the duration of connection with neighboring nodes. The more time a node remains connected with its neighbors, the higher will be the trust established with them. Therefore, mechanisms for trust establishment are categorized as follows.

- Direct establishment: Trust is established through direct communication between nodes.
- Indirect establishment: Trust relationships are transferable as nodes share the information about their trust relationship with other nodes.

Hybrid establishment: Trust is established by combining both direct and indirect mechanisms.

3. ATTACKS IN VANETS

In VANETs, it is important to account for non-cooperating entities because malicious nodes can deliberately mislead other vehicles by disseminating false traffic information and degrade the network performance. In this section, possible attacks in VANETs[13] are discussed..

- Denial of Service Attack: In this type of attack, the attackers attempt to make the communication channels unavailable or take control of vehicle's

resources. It can degrade the network's performance and also affect driver's safety, especially when safety-related application is affected. For example, if the attacker creates a massive network traffic on the road, when accident occurs, the approaching vehicles are prevented from receiving warning messages due to the denial of service attack.

- Message Suppression Attack: In this type of attack, an attacker selectively drops messages from the network. The dropped message could be safety related messages or critical information for the receiver. Also, the attacker may attempt to replay the dropped message later and mislead the drivers.
- Fabrication Attack: In this type of attack, an attacker attempts to transmit fabricated messages into the network. The messages sent by the attacker could contain false traffic information or fake identity information. It can also contain false warning messages and certificates.
- Alteration Attack: In this type of attack, an attacker attempts to alter existing messages. The attacker can change the content of the message or delay the message transmission.
- Replay Attack: In this type of attack, an attacker attempts to send an earlier message again to take advantage of the situation at the time of sending. Since a message is replayed, this is called replay attack.
- Sybil Attack: If fake information is reported by a single malicious vehicle, it is not sufficient to be convinced and trusted. Some applications require several vehicles for the same information to be accepted as true. In this type of attack, a single malicious vehicle acts as multiple vehicles by creating a large number of pseudonyms. Since the vehicles trust the fake information and make decisions based on the fake information, preventing this type of Sybil attacks is crucial in VANET.
- Privacy Attack: If vehicles are required to have a unique identity in the messages transmitted, Sybil attack may be prevented. However, if such unique identity is used, an observer may be able to identify the vehicle by tracking the messages it transmits. Hence, privacy issues also need to be addressed while protecting Sybil attacks.

Secure Routing and Data Dissemination in VANETs

Security aspect of VANET infrastructure is a very important and has not been dealt with the attention it deserves. Because of the impact on the safety and security of passengers in the vehicles, designing protocols for delivering messages securely is important.

In addition to the communication device, many authors assume that each vehicle is equipped with a reliable positioning device (e.g., a Global Positioning System), so it can obtain accurate location and time information. To ensure that all security constraints are carefully handled, we assume a scenario where the adversaries can intercept any message in the VANET.

Because of their potential impact on the safety and security of human being in the vehicles, designing protocols for exchanging messages securely is important. The security objectives are authentication, non-repudiation of signaling packets, protecting conditional user privacy, detecting and correcting malicious data, and excluding misbehaving nodes from route discovery while messages are transmitted efficiently.

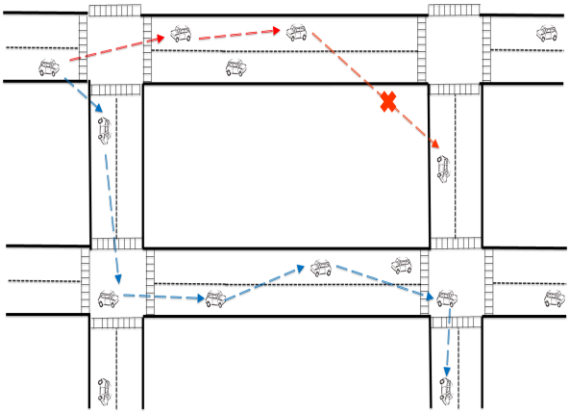

Figure 1: VANET Routing

4. AODV PROBLEM STATEMENT

When a vehicle senses an incident such as accident, bad road condition due to weather, traffic jam, etc., it needs to send that information to vehicles in appropriate regions so their drivers (or vehicles themselves, if they are self driving) can take appropriate action. When such messages are sent, the integrity and authenticity of the messages sent by the vehicles should be verified while at the same time the anonymity of the senders of these messages should be preserved. i.e, the identities of the vehicles (or drivers) should not be revealed to any other vehicle (driver). The expected method should be scalable. The protocol should take into consideration the limited computation power of the OBUs. Also, retaining satisfactory security is essential as

attacks to the network can be very dangerous and life-threatening to drivers due to the nature of messages in VANET, so the protocol should prevent possible attacks. If a RSU[15] is not within the transmission range of vehicles sending messages, the original messages are forwarded to the RSU through other vehicles, hence the protocol should be robust against malicious nodes in the network[14].

5. CONCLUSION

VANETs are likely to be deployed in the near future due to the various features they are likely to enhance the driving comfort of drivers as well as passengers traveling in the vehicles. Moreover, due to the widespread adoption of vehicle communication, vehicles participating in VANETs are likely to utilize clouds to store information as well as retrieve information. In this dissertation, we addressed some of the issues related message dissemination in VANETs; we also presented an architecture for Vehicular communication.

REFERENCES

[1] Ghassan Samara and Yousef Al-Raba'nah, "Security Issues in Vehicular Ad Hoc Networks (VANET)", International Journal of Sciences & Applied Research IJSAR, 2(4), page no. 50-55, 2015.
[2] Saif Al-Sltan,Moath M.Al-Doori'Ali H. Al-Bayatti and Hussien Zedan, "A comprehensive survey on vehicular Ad Hoc network", Journal of Network and Computer Application,Volume 37,Page no. 380-392, 2014.
[3] L Lias Kalamaras, Alexandros Zamichos, Athanasios Salamanis, Anastasios Drosou, Dionysios D. Kehagias, Georgios Margaritis, Stavros Papadopoulos and Dimitrious Tzovaras, "An Interactive Visual Analytics Platform for Smart Intelligent Transportation Systems Management", IEEE Transactions on Intelligent Transportation Systems,Volume19, Issue 2, Page no. 487-496; 2017.
[4] Yasser Toor, Paul muhlethaler, Anis Laouiti and Arnaud De La Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues", IEEE Communications Surveys & Tutorials,Volume 10 ,Issue 3, Page no.74-88, 2008.
[5] Adnan Nadeem and Michael P.Howarth, "An intrusion detection & adaptive response mechanism for MANETs", Elsevier, Volume 13, Page no. 368-380, 2014.
[6] Richard Gilles Engoulou Martine Bellaïche, Samuel Pierre and Alejandro Quintero, "VANET security surveys", Elsevier, Volume 44, Page no.1-13, 2014.
[7] Khaleel Mershad, Hassan Artail, Mario Gerla, "ROAMER: Roadside Units as message routers in VANETs", Elsevier, Volume 10, Issue 3, Page no. 479-496, 2012.
[8] Sunilkumar S. Manvi and Shrikant Tangade, "A survey on authentication schemes in VANETs for secured communication", Elsevier, Volume 9, Page no. 19-30, 2017.
[9] Muhammad Tufail Hashmi,Awais Adnan, Fazle Hadi and Muhammad Zubair, "Localized data fusion model for VANETs using GPS and non-GPS system", IEEE, 2017.
[10] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil and Anis Laouiti, "VANet security challenges and solutions:A survey", Elsevier, Volume 7, Pageno. 7-20, 2017.
[11] Chaker Abdelaziz Kerrache, Carlos T. Calafate, Juan-Carlos Cano, Nasreddine Lagraa and Pietro Ma, "Trust Management for Vehicular Networks: An Adversary Oriented Overview", IEEE, Volume 4, Page no. 9293-9307, 2016.
[12] Raju Barskar, Manish Ahirwar and Richanshu Vishwakarma, "Secure key management in vehicular ad-hoc network: A review", 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016.
[13] J. T. Isaac, S. Zeadally and J. S. Camara, "Security attacks and solutions for vehicular ad hocnetworks", IET Communications, Volume 4, Issue 7, Page no.894-903, 2010.
[14] Rakesh Kumar and Mayank Dave, "A Comparative Study of Various Routing Protocols in VANET", International Journal of Computer Science Issues (IJCSI), Volume8, 2011.
[15] Jun Tao, Limin Zhu, Xiaoxiao Wang, Jian He and Ying Liu, "RSU deployment scheme with power control for highway message propagation in VANETs", 2014 IEEE Global Communications Conference, 2014.