Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey of Various Security Techniques in VANET

Rashmi Raiya*
M TECH Student of ECE Department,
Shri Baba Masthnath College Of Engineering, Rohtak
India

Shubham Gandhi
Associate Professor of ECE Department
Shri Baba Masthnath College Of Engineering, Rohtak
India

Abstract— Vehicular networks (VANETs) are a growing research area with a large number of use cases. Foreseen applications include safety applications, traffic efficiency enhancement and infotainment services. VANETs connects vehicle into a huge mobile ad hoc network to share information on a larger scale. The characteristics of VANET pose both challenges and opportunities in achieving security goals. Providing security to VANET is important in terms of providing user anonymity, authentication, integrity and privacy of data. In this paper we have discussed the various techniques which associated with the security, reliability and confidentiality of the disseminated data in VANET.

Keywords— VANET, security issue, key management techniques

I. INTRODUCTION

With the rapid development of wireless technologies, peoples are starting to enjoy wireless access everywhere, from cafe, to hotels, to airport; wireless access is even being seen in vehicles on the move. Recently, car manufacturers and telecommunications industries have teamed up to equip every car with wireless technologies; these technologies can not only bring various information technology services to vehicles on the move but also improve road safety and traffic efficiency. Cars that are equipped with wireless communication devices and road side infrastructure can form a huge self-organised communication network called a vehicular adhoc network (VANET). Specifically, a VANET is a dynamic collection of network vehicles that communicate with each other or nearby roadside units (RSUs), using a dedicated short range communication technique [1]. These vehicles are equipped with wireless on-board unit (OBUs), which perform this communication.

The VANET provides a ubiquitous computing environment to drivers and passengers and enables numerous services through a variety of vehicle applications. Applications, such as emergency-braking warning, are made possible by communication between vehicles. By using VANETs, travellers can achieve improved driving safety and comfort. For example, each vehicle user may periodically broadcast its proximal traffic information to others, enabling them to take early action to avoid car accidents. Moreover, nearby vehicle user van share specific information with each other, such as road conditions, tourism information, music, movie files, or hotel information, making themselves more comfortable and knowledge during their journeys. Indeed due to their enormous potential and social impact, VANETs have drawn considerable research attention from both academia and industry, and many prototype applications have already been developed; however, before implementing these promising applications, particularly safety related ones, VANET-related security problems must be addressed and resolved.

II. SECURTY SERVICES IN VANET

Security is an important issue for ad hoc networks especially for security sensitive applications. To ensure an ad hoc network, we need to consider the following attributes criteria to measure security which includes availability, confidentiality, integrity, authentication and non-repudiation.

A. Availability

The availability deals with the network services for all nodes comprises of bandwidth and connectivity [2]. In order to encounter the availability issue, prevention and detection techniques using group signatures scheme has been introduced. The scheme is focussing on the availability of exchanging the messages between vehicles and RSUs. When the attack causes network unavailability, the proposed technique still survives due to interconnection using public and private keys between RSUs and vehicles.

.

B. Confidentiality

This service provides the confidentiality to the communication content. It guarantees the privacy of drivers against unauthorised observers. The most popular technique pseudonyms are used to preserved privacy in vehicular networks. Each vehicle node will have multiple key pairs with encryption. Messages are encrypted on signed using different pseudo and these pseudo has not linked to the vehicle node but relevant authority has occurred to it. Vehicle need to obtain new pseudo from RSUs before the earlier pseudo expires.

C. Authentication

Authentication is the verification of identity between vehicles and RSUs and the validation of integrity of the information exchange. Additionally, it ensures that all vehicles are the right vehicle to communicate within network. Public or private keys with CA are proposed to establish connection between vehicles. RSUs and AS; on the other hand, password is used to access to the RSUs and AS as authentication method.

D. Integrity

Data integrity is the assurance that the data received by nodes, RSUs and AS is the same as what has been generated during the exchange of message. In order to protect the integrity of the message, digital signature which is integrated with password access are used.

E. Non-Repudiation

Ensures that sending and receiving the message cannot deny ever sending and receiving the message such as accident messages. In certain fields, non-repudiation is called auditability where by RSUs and vehicles can prove have been receive and sent respectively.

Table I shows the analysis of various security services, security attacks and techniques.

TABLE II
ANALYSIS OF SECURITY SERVICES

Security Problems	**Security attacks**	**technique**
Availability	Interruption	Group signature
Confidentiality	Interception	Encryption and Decryption
Authentication	Fabrication	Certificate Authority (CA)
Integrity	Modification	Digital signature with password
Non-repudiation		Sequence number, digital signature

III. KEY MANAGEMENT TECHNIQUES

Vehicular ad hoc network is commonly used network among the vehicles in a centralized way. This network is built in order to send and receive messages from the vehicles which are present in the network. The main issue of the VANET are maintenance of the system and revocation of malicious vehicles. Therefore the various management keys have been framed to overcome the above said problems. These are:

A. *Distributed Key Management Frame*

A distributed key management framework based on group signature to provision privacy in vehicular ad hoc network (VANETs). All of the existing group signature schemes in VANETs are based on a centralized key management which preloads keys to vehicle. In this framework, since keys are distributed and the distributed keys are connected to the centralized sever [2][3]. Sending and receiving messages ends up in delay in delivering the messages security related issue in hacking the packet data and the message authentication is distance biased

This technology uses the below said techniques for this framework

1. Centralized server (or) centralized authenticator
2. Extra protocols for beyond the range
3. Group authentication

Centralized server:
Centralized server are centralized authenticator will be the roadside connected with the key distributor.
Extra protocols for beyond the range:
Extra protocol may be added for sending and receiving messages beyond the range.
Group authentication:
Group authenticator is done for the connected keys with the group leader.

B. *Shared Key Management Framework*

The author proposed the shared key management technique that has various advantages over the distributed key management system. In this framework RSU is not responsible because the key is shared among them, when a vehicle approaches another vehicle [3]. It's getting connected to the vehicle automatically without the help of RSU. But message is send from one vehicle to another vehicle needs the help of RSU.

The centralized server is not required, since the keys are shared group authentication is not necessary for transferring the information because the key them self shared the information.

In this method there is no necessity for extra protocol for the authentication beyond the range why because every participating key is given priority message authentication.

C. *Safety Message Broadcast In VANET*

In vehicular ad hoc network (VANETs), because all vehicles in range are shown as destination nodes and less time is spent for the medium access process, broadcast communication is considered a highly appropriate technique for the dissemination of safety message in such networks [4]. However the lack of request- to-send/clear-to-send handshaking and packet acknowledgment makes the communication more vulnerable to interference, thus resulting in lower communication reliability. The author presents an analytical model for the performance evaluation of safety message dissemination in VANET with two priority classes.

In this survey we consider the coexistence of periodic applications and event driven safety applications. Message that belongs to periodic applications are broadcast among vehicles, as frequently as necessary, to inform each other about their local parameters such as speed and position. On the other hand, a message that belongs to event-driven applications is a safety message that I generated by vehicle, which detects or experiences a hazard or an unusual event. In the network, a high ratio of traffic will consists of message is generated by first type of application which may reduces the resource availability for second type of messages however safety message are time critical, they have to be given higher priority compared to message of periodic application.

It is a well known phenomenon that increasing the transmission range increases the network connectivity. On the other hand it increases back-off time for the messages, which result in a higher multihop transmission delay. Furthermore, the traffic of frequent low-priority applications should be controlled to satisfy the required delay bounds for the immediate high priority traffic.

D. Efficient Cooperative Message Authentication In Vehicular Ad Hoc Networks:

In the survey of cooperative message authentication scheme for VANETs. Vehicle users can cooperatively authenticate a bunch of message-signature pairs without the direct involvement of a TA (Trusted Agent). Trusted security mechanisms and protocols have been recently developed to ensure secure privacy-preserving vehicular communications [5][1]; they can be classified as public key cryptography (PKC)-based or secret key- cryptography (SKC)- based solutions.

In addition, the free riding attacks without authentication efforts, which are launched by selfish vehicle users, can be also effectively resisted through an evidence- token approach; the frree riding attacks with fake authentication efforts can be prevented by enforcing vehicle users to output their authentication proofs. The TA adjust the valid period of tokens for each vehicles user based on the collected evidence, thereby periodically controlling vehicle users' cooperation capabilities.

IV. CONCLUSIONS

This paper has briefly introduced the vehicular ad hoc networks, security services and various techniques. It also deeply specify the message authentication schemes such as broadcast message dissemination and efficient cooperative message authentication using PKC and SKC. For secure message dissemination various techniques have been identified and discussed to solve the security issues. This survey includes the five security services and techniques have been analyzed to its security problems

REFERENCES

[1] Yong Hao, Yu Cheng and Chi Zhou "A Distributed Key Management Framework With Cooperative Message Authentication in VANET", International Journal On Selected Areas In Communications, vol.29, no.3, March 2011.

[2] G.Sasikala and K.S.Dhanlakshmi "Key Management Techniques for VANET", Special Issue of International Journal of Computer Applications (0975-8887) on International Conference on Electronics, Communication and Information System (ICECI 12).

[3] Mehndi Khabazian, Sonia Aissa and Mustafa Mehmet-Ali "Performance Modeling of Safety Messages Broadcast in Vehicular Ad Hoc Networks", IEEE Transactions On Intelligent Transportation Systems , volume 14-no.1, March 2013.

[4] Xiaodong Lin, Xu Li "Achieving Efficient Cooperative Message Authentication in Vehicular Ad-hoc Network",IEEE Transactions on Vehicular Technology, volume 62, no. 7, September 2013.

[5] Kamini and Rakesh Kumar"VANET Parameters and Applications: A Review", GJCST Computing Classification, volume 10, issue 7, ver. 1.0, September 2010.

[6] Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl," Graph-Based Metrics for Insider Attack Detection in Multihop Data Dissemination Protocols", IEEE Transactions on Vehiicular Technology, Volume 62, No. 4, May 2013.

[7] Maria ELSA Mathew and Arun Raj Kumar p.," Threat Analysis and Defence Mechanisms in VANET", International Journal of Advanced Research in Computer Science and Software Engineering, 3(1), January-2013.

[8] Ahmed Yusri Dak, Sadish Yahya and Murizah Kassim,"A literature Survey on Security Challenges in VANET",International Journal Of Computer Theory And Engineering", Volume 4, No. 6, December 2012

