Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Overview of Security Challenges and Needs in Vehicular Ad-Hoc Networks

Menal Dahiya
Department of Computer Science, Maharaja Surajmal Institute,
Delhi, India

Abstract— Wireless communication has been gaining fast recognition in the current years. Selection of standards depends on the ease of use and level of security it provide. The era of vehicular ad-hoc network (VANETs) are receiving increasing attention from academia and deployment effort from industry. Vehicle Ad-hoc networks (VANETs) is important form of mobile ad-hoc networks. The VANETs provide a smart transmission between vehicles and also among vehicle and roadside infrastructure. VANETs too have few prominent and visible problems like other technologies. Security amongst is the biggest problem. Therefore, working on security protocols in VANETs is essential. This paper discusses the security problems that necessarily are excel to make VANETs almost practical.

Keywords— RSU, Security Challenges, Security Protocols, VANETs, Wireless Communication.

I. INTRODUCTION

VANET is a wireless Ad-hoc network where the node, one of two vehicle and road side infrastructure (RSU) can give and exchange information for meaning of inquiry or allocation. This can be reached by permitting nodes to connect inside fixed distance of 2-10 kilometres in order to transfer message about traffic conditions [1]. VANETs can assist in bringing safety services and bettering the driving exposure. Also, entertainment alternatives can be presented to customers like TracNet system and KHV to give internet access in vehicles. The variety of applications are compelled by the reality that VANETs to eventually consider a form of ubiquitous network which determine to give many services with a distinct access point. Today communication technologies in VANETs are based on existing protocols like IEEE 802.11 with its different improvements [2]. Few applications of VANETs like "Salik" which is based on radio frequency identification (RFID). Still, these techniques bring out some temporarily issues which are intolerable. As a result an IEEE project to support a new improvement to the 802.11 standard that will enhance communication for such network is in progress. The new standard popularly known as IEEE 802.11p is based on DSRC but with an inclusion of wireless access for vehicular environments (WAVE). WAVE will support both vehicle-to-vehicle and vehicle-to-Road side infrastructure transmission in VANETs. VANETs to be used in the future they must provide adequate level of security and privacy to the user. These features of the network are of principle significance as they influence person's safety and may compromise their privacy if not correctly addressed [3]. The future aim of VANET security protocols is to give a vehicular communication network that is intelligent to oppose actions, attacks and give the best likely level of node privacy. The basic architecture of VANETs is shown below in fig.1 [4].

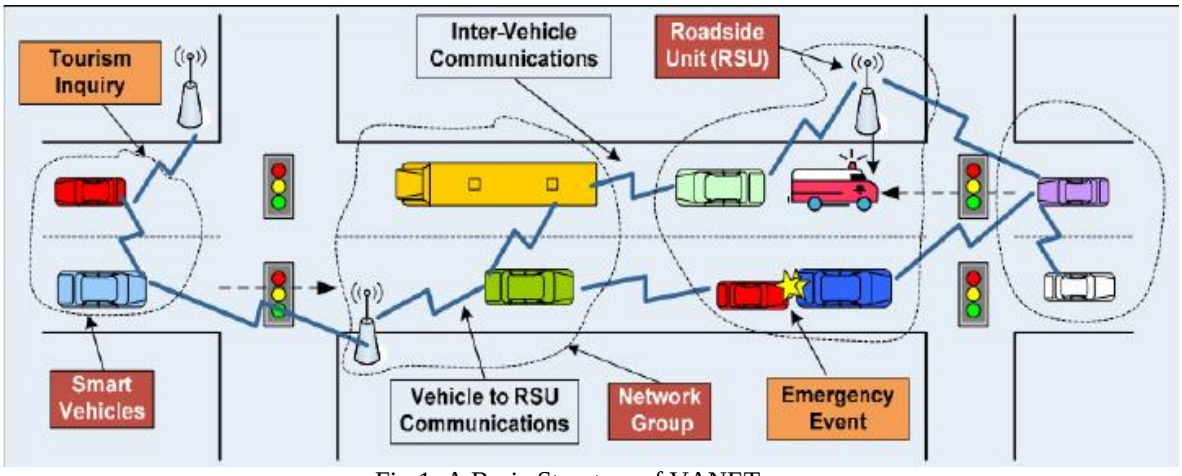

Fig.1: A Basic Structure of VANETs.

Section 2 of the paper addresses the challenges that are faced in VANETs. Section 3 discusses security needs. In last, we will cover the future research directions and conclusion.

II. CHALLENGES FACED BY VANETS

The final aim of the VANETs is to improve the driving experience by providing various measures of safety while driving. Though, in order to reach this aim, few challenges necessarily be faced. These challenges include [5]:

A. Real-Time Guarantees

VANET applications are time based where safety related information like accident warning, hazard warning, collision avoidance etc. should be delivered with 100ms transmission delay. So to achieve real time, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

B. Mobility

Vehicle make connection through their way with other vehicles that maybe faced before, and this link ends for only few seconds as every vehicle goes to their route and these two vehicles may never face again. So securing mobility challenges is difficult. Due to high mobility protocols can't be contact based and most of the communications among nodes that are not in any way communicated earlier, thus knowledge based scheme should be introduced so that they lean to know about each other's behaviours.

C. Liability

Liability will give a favourable circumstance for legal analysis and this information can't be refused like case of accident, on other hand privacy must not be breached and every driver must have the ability to keep his private data i.e. identity, toll receipt, driving path etc from others.

D. Authentication

The significance of certification in vehicular ad-hoc network is to guarantee that the data are transmitted by the authentic nodes but maximum of the drivers desire to maintain the data shielded and personal.

E. Incentives

Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET [6]

III. SECURITY NEEDS IN VANETS

Any security protocol must make secure that fundamental necessity are achieved in VANETs. These needs include [7]:

A. Availability

Availability requires that the information must be available to the legitimate users. DoS Attacks can bring down the network and hence information cannot be shared.

B. Authentication

Authentication is a major necessity of VANETs as it make secure that the data are transfer by the authentic nodes and hence attacks done by the greedy drivers or the other attackers can be weakened to a greater magnitude.

C. Non-Repudiation

Here a node cannot turn down that he/she will not transmit the data. It may be important to determine the accurate order in crash restoration.

D. Real-Time Guarantee

It is important in VANETs that lots of safety associated applications depend on strict time lines. This can be built into protocols to ensure that the time sensitivity of safety related applications like collision avoidance in met [8].

E. Privacy

The privacy of a node against the unauthorized node should be protected. This is required to eliminate the massage delay attacks.

F. Confidentiality

It make secure that the text of information is kept classified from unauthorized nodes.

G. Integrity

It make secure that information are not altered in passage and the information received by the drivers are not fictitious.

IV. CONCLUSIONS

Vehicular Ad-hoc network is an emerging wireless networking concept of the wireless ad-hoc networks which provide safety and security to drivers and passengers if applicable properly. Security in VANETs is a major challenge

and a hot topic for research among researchers. VANET provide convenience and several applications to the system. This paper concludes the security challenges and the fundamental requirements for VANETs.

REFERENCES

[1] Bhoi K. S and Khilar M. P., "Vehicular Communication: A Survey," The Institution of Engineering and Technology, Vol.3, Issue.3, pp. 204-217, 2013.

[2] Toor Y. et al., "Vehicle Ad Hoc Networks: Applications and Related Technical issues," IEEE Communications surveys & Tutorials, Vol.10, Issue.3, pp. 74-88, 2008.

[3] Mokhtar B and Azab M, "Survey on Security Issues in Vehicular Ad-hoc Networks," Alexandria Engineering Journal, Vol.54, Issue.4, pp. 1115-1126, 2015.

[4] La H. V and Valli C. A., "Security Attacks and Solutions in Vehicular Ad-hoc Networks: A Survey," Vol.4, Issue.2, pp. 1-20, 2014.

[5] Moustafa H and Zhang Y, "*Vehicular Networks: Techniques, Standards, and Applications*," CRC Press. 2009.

[6] Raw S. R., Manish Kumar M and Singh N., "Security Challenges, Issues and Their Solutions for VANET," IJNSA, Vol.5, Issue.5, pp. 95-105, 2013.

[7] Chaubey K. N, "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study," International Journal of Security and its Applications, Vol.10, Issue.5, pp. 261-274, 2016.

[8] Gaikwad G. P and Patil N, "Survey on Vehicular Ad-hoc Networks Security," IJIRCCE, Vol.5, Issue.1, pp. 725-731, 2017.

