International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

A STUDY ON SECURITY SYSTEM OF VEHICULAR AD HOC NETWORK

Anirban Patra, Samayita Sarkar, Anirban Ghosal

[1,2,3]*Assistant Professor; JIS College of Engineering, Kalyani, Nadia, West Bengal (India)*

ABSTRACT

Vehicular Ad hoc Networks (VANET) is the subclass of Mobile Ad Hoc Networks. It is the most advanced technology that provides Intelligent Transportation System in wireless communication among vehicles to vehicles and road side equipment to vehicles. Vehicular network is a growing research area with a large number of use cases. VANETs connects vehicle into a huge mobile ad hoc network to share information on a larger scale. Vehicular Ad Hoc Networks is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. Providing security to VANET is important in terms of providing user authentication, integrity and privacy of data.The security and privacy issues of VANETs must be addressed before they are implemented. In this paper, important points in VANET security are studied.

Keywords: Vehicular Ad Hoc Network, Attack,Security, Authentication, Authorization

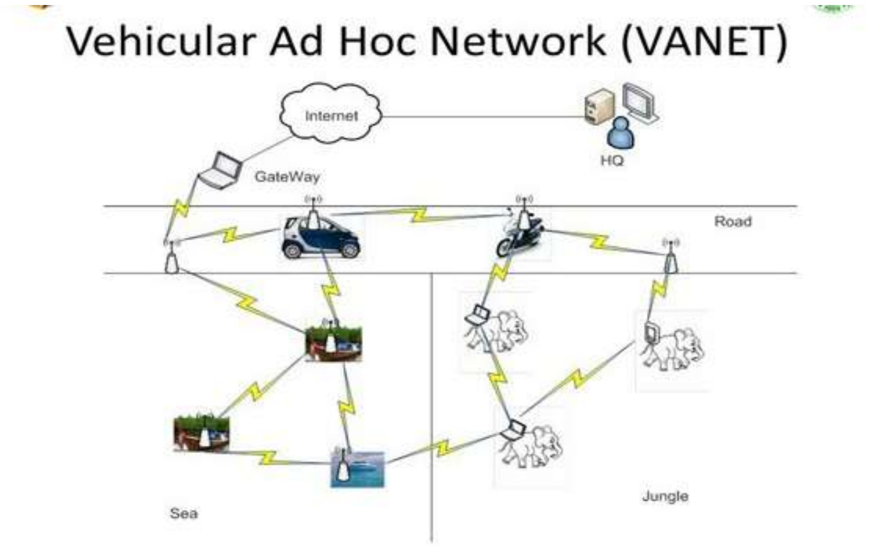
I. INTRODUCTION

Vehicular Ad hoc Network is an emerging networking system which is used widely in nowadays. But just like other advanced networking system it is not prone to attack. VANET is an application of mobile ad hoc network. More precisely a VANET is self-organized Network that can be formed by connecting vehicle aiming to improve driving safety and traffic Management with internet access by drivers and programmers

Security, has always been an issue in vehicular networks which must be seriously considered and a security infrastructure has to be designed and implemented in such networks. An attacker can inject false and invalid traffic messages into the network to distract drivers from choosing a specific route, or can use the network to determine a driver’s location or identity. On the other hand, by gaining unauthorized access in network, an attacker can gain the control of critical components of a vehicle and cause irreparable damage to the vehicle or its passengers. One of the main challenges in VANET is to route the data efficiently from source to destination. Designing an efficient routing protocol for VANET is difficult task.

II. ATTACKS IN VANET

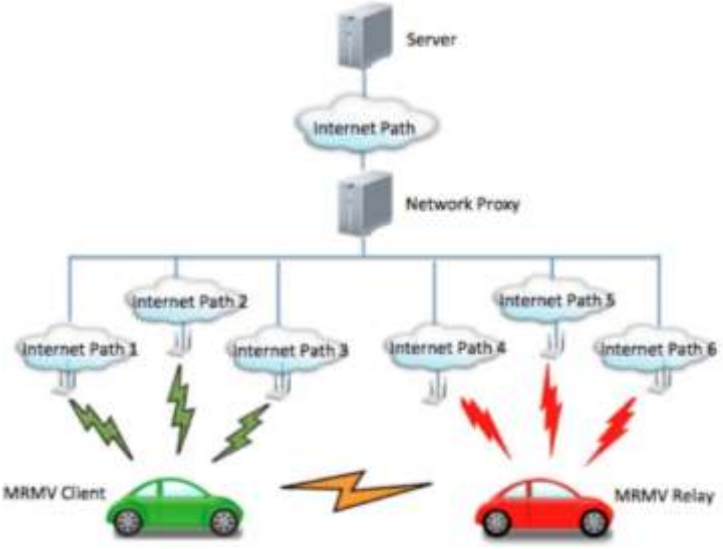
- Impersonate: Perform by active attacker assuming identity and privilege of an authorized vehicle
  Misuse network resource that may not be available to it under normal circumstances hence disrupt normal functioning of the networkAttacker may be insider or outsider.Multilayer attack as attacker can exploit either network layer, application layer or transport layer
- False attribute possession: Steals some attribute from legitimate user and behaves as a legitimate user SybilAttacker uses different identities at the same time while sending multiple messages to other different vehicles
- Session hijacking: Most authentication process start after starting session hence easy tohijack session after establishing connection



III. ATTACKERS IN VANET

- Insiders: Authentic members of network, communicate with other members of the network
- Outsiders: Not authenticated for direct communication with other members of the network
  Intruders and hence limited capacity to attack
- If the attacker is a member node who can communicate with other members of the network, it will be known as an Insider and able to attack in various ways. Whereas, an outsider, who is not authenticated to directly communicate with other members of the network, have a limited capacity to perform an attack .
- Malicious Attacker:Uses various methods to damage the member nodes and the network without looking for its personal benefit
- Rational Attacker: Expects its own benefit from the attack

A malicious attacker uses various methods to damage the member nodes and the network without looking for its personal benefit. On the contrary, a rational attacker expects its own benefit from the attacks. Thus, these attacks are more predictable and follow some patterns.



IV. CHALLENGING ISSUES IN VANET

Technical Challenges:The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET.

Some challenges are given below:

• Network Management: Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as rapidly as the topology changed.

• Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

• Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

• MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

• Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

Social and Economic Challenges Apart from the technical challenges to deploy the VANET, social and economic challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. Conversely, consumer appreciates the warning message of police trap. So to motivate the manufacturer to deploy VANET will get little incentive.

V. CONCLUSION

Vehicles can communicate with the roadside communication infrastructure and also among each other to improve road safetyVehicle not only an information source or sink, but also information distributor Communication services enable a wide range of applications, ranging from road safety and traffic efficiency, driving comfort and infotainment. The technologies used for vehicular networks are still not mature and will probably not be implemented in the immediate future. The opportunities that a VANET presents are unlimited. The future introduction vehicular networks offer a tremendous opportunity to increase the safety of the transportation system and reduce traffic fatalities.

REFERENCE

Journal Papers

[1]AnkitaAgrawal, AditiGarg , NiharikaChaudhiri , Shivanshu Gupta, DeveshPandey , Tumpa Roy ; Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper ;International Journal of Emerging Technology and Advanced Engineering ; (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013)

[2] SabihurRehman , M. Arif Khan, Tanveer A. Zia, LihongZheng ; Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges ; Journal of Wireless Networking and Communications 2013, 3(3): 29-38

[3] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and RongfangBie; Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends ; International Journal of Distributed Sensor Networks ;Volume 2015 (2015), Article ID 745303

[4] VinhHoa LA, Ana CAVALLI ; Security Attacks & Solutions in Vehicular AD HOC Networks: A Survey; International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014

Conference Papers

[1]Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures ; Security Analysis of Vehicular Ad Hoc Networks (VANET) ; Second International Conference on Network Applications, Protocols and Services , 2010

[2] I. A. Sumra ; H. Hasbullah ; J. l. A. Manan; VANET security research and development ecosystem; National Postgraduate Conference (NPC), 2011