Avoiding Prankster Attack in Case of Selfish Driver Using the Location Aware Fixed Nodes - A Review

Namrata Singh*1, Khushneet Kaur*2

*1 Research Scholar ECE Department, Doaba Institute Of Engineering &Technology Kharar(Mohali)Punjab,India
*2 Associate Professor ECE Department, Doaba Khalsa Trust Group Of Institute Rahon(Nawashar)Punjab,India

Abstract -- VANET Security is a popular research area and concerns with the automatically driven vehicles. VANETs are prone to number of security breaching methods. These security breaches can be categorized as Replay Attack, Denial of Service, Fabrication Attack, Prankster Attack, etc. These attacks can cause massive traffic congestion, accident or to hurt large number of people with terrorism activities. Prankster Attack is the one, which is launched by sending the false information to other vehicles, which can cause traffic congestion, accident or terrorism activities. In this paper, we are proposing a method to prevent the prankster attack. This attack can be prevented by implementing fixed and location-aware nodes across the road, which can compare the GPS coordinates with its coverage area to make the decision that vehicle is transmitting true or false information.

Keywords- Prankster attack, VANET(vehicular ad hoc network)

I. INTRODUCTION

A vehicular ad hoc network forms a network using moving nodes to establish a mobile network. In VANET, the cars which take part in a network is turn into wireless router or node. These nodes form a wide range network. If signal range of that particular node is not there then the other node can take place of that node. The first system which use this technology is police and fire system for safety purpose to communicate with each other. Vehicular network is deployed to provide efficiency, safety and security of public transportation system. It establishes a new mobile technique and services for travelling public. In comparison to today traffic management the future intelligent traffic management offers various advantages to public. The vehicle can sense their location and share information with each other by deploying VANET. By using this type of facility it reduces the traffic congestion. The deploying of VANET network as compared to conventional system such as UMTS, LTE, Wi-Max has several advantages like low cost of implementation maintenance self organisation. The main purpose of VANET is to provide passenger safety and comfort by establishing a vehicular communication system that provide quick and cost efficient distribution of data.

VANET Security is the most critical issue. VANET is prone to hacker. The VANET security is compromised in many ways. In this review paper we are discussing about VANET security. The VANET system is attack by the PRANKSTER. In case of PRANKSTER attack in VANET all the system get affected. In PRANKSTER attack hacker provide wrong information to traffic nodes. VANET is originate from mobile ad hoc network by the development in the wireless communication. It has made road vehicle communication and inter vehicle communication to give birth to the VANET. Every node is connected with each other and they can move with in the network coverage. Any node can be vehicle or road side unit and each node is communicate with each other. The movement and self organization of nodes helps to differentiate between MANET and VANET. The other difference between these network is that VANET nodes are capable of recharging their battery power again and again but MANET nodes cannot be recharged their battery power.

It provide traffic guidance, location and position based services and security information. In collision avoidance application vehicle to vehicle and vehicle to infrastructure communication can prevent injuries and save many lives. After observing an accident, a vehicle reduces its speed significantly and it will propagate its location to the other vehicles and emit alarm to its drivers. So the drivers can get the alarm and can take decision for his safety.

II. LITERATURE REVIEW

Ghaleb F. et. al. has proposed the mechanism for security and privacy enhancement in VANETs Using Mobility Pattern[1]. In this paper, the authors have addressed the issue of mobility pattern based misbehavior detection in VANET platform. The authors have classified the attackers as insider and outsider. Samara G. and associates have conducted a survey on the security analysis Of VANETs[2]. In this paper, the
authors have simulated various type of security problems and challenges of VANET platforms. The authors have also discussed the solution to solve these challenges and problems by using RSU via DSRC. Seuwou P have developed an effective security as an ill-defined problem in VANETs[3]. Qian yi et.al have conducted a survey on the performance of secure MAC Protocol for vehicular networks[12]. In this paper the authors have proposed an overview on a QoS based secure MAC Protocol for vehicular networks. Javed M.A. et.al have proposed a Geocasting technique in an IEEE802.11p based vehicular Ad hoc network for road traffic management[4]. In this paper he proposed the geocasting packet transmission technique to transfer safety message in a vehicular network. Hung c.c. with his co-researchers have developed a new Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks[5]. They have stated that traditional ad hoc routing protocols are not well suited for highly dynamic vehicular networks. In this paper they have proposed new Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing for HVN. Dias A.J. et.al. proposed a Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks[6]. Sumra A.I. et.al. proposed the Trust Levels in Peer-to-Peer (P2P) Vehicular Network[8].

III. PROBLEM FORMULATION

VANETs (Vehicular Ad-hoc Networks) are the emerging network technology for the moving vehicles and emerged as a popular research area. This emerging vehicular network technology is taking the world into a new age of automatically driven vehicles. These automatically driven vehicles will communicate with other vehicles digital medium of VANETs. This digital medium is prone to hacking and several attacks can take place in the VANETs. These attacks can cause major security issues, accidents, traffic congestion, etc. So, before the VANETs come into the real time application, all those threats must be reviewed and effective solutions should be produced to fill those gaps in VANETs. The major attacks on VANETs are DoS, Fabrication Attack, Sybil Attack, Selfish driver, Replay Attack, Malicious Attack, etc. All of these attacks cause some kind of chaos in the movement of vehicles. DoS (Denial of Service) Attacks are caused by flooding of many packets and result of which is communication hurdle between the vehicles. Fabrication Attack is the one in which vehicle sends the false information about its location. Alteration attack is the one when hackers edit the existing data in the database which cause a great traffic mess. Prankster Attack is when some hacker causes a false virtual traffic information and forces the vehicles to move into another direction from their pre-decided path. Selfish driver or Terrorist can propagate false information in the VANET and then as a result the vehicle will change their lane or direction, which can cause a traffic jam, unexpected turn or accident, which can further doctor the security of the public or VIP vehicles. In this research we are addressing the issue of Prankster Attack in case of Selfish Driver.

IV. PROPOSED SYSTEM

In this research, we are proposing a VANET security method to protect the prankster attack in case of selfish driver. In prankster attack, selfish driver propagates the false information in the cluster, which move vehicles into another direction or stop them on road side. Usually, selfish driver launches this attack to benefit himself/herself and to make his/her way clear. Selfish driver (Terrorist) can also avail prankster attack to create a traffic mess, where he can blast and can cause a larger number of causalities. To prevent this attack, location aware fixed nodes will be used in our proposed method. Location aware fixed nodes will be aware of their coverage area in perspective of the GPS coordinates. Hence, if the vehicle (Assume CAR-X) travelling in their area will propagate its false location, which is out of the coverage area of the fixed node, it will detect the false information. Then, discard the false information, and broadcast a message in the network that CAR-X is a malicious vehicle. The fixed nodes will communicate with each other. Assume that fixed nodes A, B and C are aligned from left to right. So if a vehicle will enter from node A to node B, it is detectable that vehicle is moving into the right side direction and vice versa. So our method will also be able to detect the correct direction of the movement of the vehicle. Hence, a vehicle will not be able to propagate the false information about the direction of its movement.

V. METHODOLOGY

We will start our research project by conducting a detailed literature review on the prankster attack in case of selfish driver in VANETs to know the problem in detail. Then, a detailed security mechanism would be designed to prevent the prankster attack in VANETs. The simulation would be implemented using Network Simulator (NS2). The obtained results would be examined and compared with the existing security mechanism to address the similar issues.

VI. REFERENCES


[3] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma “Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)”.


