International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 14-17(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Roadside Traffic Management Unit to Mitigate Prankster attack in Vanet Cluster

Deepak Singla*, Gurbinder Singh Brar** and Shivani Sachdeva*
**Department of Computer Science Engineering, AIET, Faridkot, (PB), INDIA*
***Assistant Professor, Department of Computer Science Engineering, AIET, Faridkot, (PB), INDIA*

(Corresponding author: Deepak Singla)
(Received 04 October, 2015 Accepted 04 November, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: VANETs are the networks used to mitigate the chaos caused by the traffic and lowers the fear of collision in the traffic movement on the roads. VANETs are also being used for the automatically driven vehicles in the controlled environments. Whereas the human vehicles use the VANETs for extra facility, the automatically driven vehicles completely depend upon the VANETs. Any incursion in the VANETs by hackers can cause major accidents or traffic chaos. A popular technique known as prankster attack is used by militants to plot attacks to cause more damage as possible or by selfish drivers to make their way clear. In this paper, we have proposed a strong security framework to mitigate threats caused by prankster attack by using road side traffic management unit (RTMU). The RTMU is using various mathematical computations to detect the abnormality in vehicle moment to detect the prankster attack. The mathematical equation programmed in the RTMU are used to determine the distance between the vehicle, normal/abnormal moment, displacement (time to distance based comparison) and fake nodes created by prankster attack to take advantage. All of the nodes in the scenario are GPS location aware nodes and sharing their location actively with RTMU. RTMU is using mathematical formula of circle to determine the distance between two points and to find the node location within its transmission range. If node is not in the transmission range, but able to propagate its location to the RTMU, it is marked as fake node and all other nodes in the cluster are updated with the information of fake node, which facilitates the smooth traffic movement in the cluster. The results have shown the effectiveness of the proposed model to mitigate the prankster attack and facilitate smooth traffic movement.

Keywords: VANET security, Prankster attack, Roadside traffic management unit, Roadside unit

I. INTRODUCTION

The most important information in a vehicular ad hoc network is vehicle position. Pranksters and malicious attackers change the original packets into fake packets and damage the VANET. The hallucination of a traffic jam before choosing the other route for his betterment may generated by the attacker. Mobile ad-hoc network forms a vehicular ad-hoc network which provides communication among nearby nodes, between the nodes or nearby fixed nodes which is called road side traffic management units (RSU). VANETs have different characteristics as compare to the MANETs such as quick change in topology, large scale, variable network density, no power constraint. The architecture of VANET is generated for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) which are placed on the road side and onboard unit (OBU) installed in vehicles. Some sensors are also installed on the cars for collecting information of road.

The other harmful attack is Sybil attack. In this, an attacker can generate different identities either by stealing identities or by fake new identities. Advanced cruise control system uses on- board radar. It is natural for the purpose of increasing the security of the information which flow in the VANET to enlist the help of these devices. The attention all over the world has been attracted by the concept of network car, with the advancement in wireless communications technology. When the attacker takes control of the vehicle's resources or there is congestion in the communication channel used by the vehicular network, denial of service attack is happened, so it prevents critical information from arriving. If it has to depend on the application's information, it also enhances the danger to the driver. Denial of service is a type of attack in which flood of packets are transmitted to a particular node, so that node connection get break down from the entire network.

We can also called VANET as wireless access in vehicular environment (WAVE) which supports intelligent transportation system (ITS) via dedicated short range communication (DSRC). Two types of communication present in VANETs are node to node (N2N) and node to infrastructure (N2I). The on board units (OBU) exist in vehicles which consist of GPS, omni-directional antennas and sensors for N2N communication. N2I communication is also performed by vehicle with roadside infrastructure, that exist within a fixed distance from others depend on the communication range of the road sides nodes ,that are also called road side units(RSUs). RSU conduct information to other RSU via wired or wireless medium. To send emergency and real time information the N2N communication can be used.

Security requirement such as integrity, confidentiality, security should be followed by the VANET since it supports emergency real time application & also deal with life critical information. Security attacks like Denial of Service, Sybil attack, wormhole attack affect the security of the drivers and nodes it compromises traffic safety, which leads to loss of the lives. Multi-hope multicast is utilized by the inter-vehicular communication configuration to transmit traffic related information. Vehicles need only be concerned with activity on the road ahead and not behind in intelligent transportation system. Native broadcasting and intelligent broadcasting are the two messages forwarding in inter- vehicle communication.

Broadcast messages are sending by the vehicles periodically, in native broadcasting. On the reception of the message, if the message has come from the car behind it, that message is ignored by the car. The disadvantages of the native broadcasting method is, large number of information are created that enhances the information collision which results in enhancing the delivery time. Intelligent broadcasting handles the problems which are in- built in the native broadcasting by reducing the messages for a given emergency event. The single hop broadcast is represented by the node to roadside communication configuration where a broadcast message is sent by the roadside unit to all equipped node in the neighbourhood. High bandwidth link between nodes and roadside units are provided by the node to roadside communication configuration.

The attacker propagates fake traffic information in the cluster and forces the nodes to move into different direction from their actual path. False information in the VANET can be propagated by the terrorist or selfish driver, therefore their direction will be changed by the by the vehicle, which can cause traffic congestion or accidents. In this paper, the issue of prankster attack in case of selfish driver are being addressed and the new technique based on roadside traffic management unit (RTMU) has been used to mitigate such attacks.

II. LITERATURE REVIEW

Ghaleb *et al.,* have worked on the mechanism for security and privacy enhancement in vehicular ad-hoc network. They have used Using Mobility Pattern to mitigate the security threats in the VANETs. They have been addressed the issue of VANET node misbehaviour by analyzing the mobility pattern in VANETs. The authors have also classified the attack origin as insider and outsider attack. Sharma *et. al*. has done a survey on security& threat analysis of vehicular ad-hoc networks. Under this research, the authors have analyzed different types of VANET security problems and challenges by simulating various security threats in VANET platforms. They have taken the solution to solve these challenges into account has proposed the use of RSU via DSRC to mitigate such attacks. Seuwou has proposed an effective security mechanism for ill-defined problem in VANETs. Qian *et.al.* have conducted a performance analysis on the performance of secure MAC Protocol for VANETs. Under this research, they have proposed the use of Quality of Service based secure MAC Protocol for vehicular networks. Javed. M.A. has developed a geocasting based protocol based IEEE802.11p standard for vehicular Ad hoc network to facilitate the smooth road traffic management. The authors have also proposed location aware packet transmission technique to transfer security related message in VANETs. **Hung c.c.** and co-researchers have worked upon mobility pattern aware routing for Heterogeneous VANETs. In this paper, the authors have proved that traditional VANET protocols are not sufficient for flexible and large VANETs. They authors have suggested a new technique called HVN (Heterogeneous Vehicular Network) architecture to mitigate such threats. Dias .A.J. and his associates have conducted survey on Routing Protocols for Vehicular Delay-Tolerant Networks. Sumra A.I. has suggested the different levels of trust in P2PVANETs.

III. POROBLEM FORMULATION

In this research, we have point out the security issues caused by prankster attacks in VANETs consisted of GPS based automatically driven vehicles. The attacker can launch the prankster attack in these VANET clusters and can cause traffic jams, accidents, militant activities, etc. This attack is caused by propagating the false traffic information about one to more nodes in the cluster to confuse and derail the movement of the traffic to take above mentioned advantages. The prankster attack can cause heavy threat to the life of people travelling in such vehicles. The ordinary public, VIPs or VVIPs travelling in the automatically driven vehicles can come under threat with the launch of such false information propagation attacks. We have proposed the use of roadside traffic management unit (RTSU) to mitigate the threat caused by prankster attack.

IV. EXPERIMENTAL DESIGN

In this paper, we have developed a new security framework to mitigate the prankster attack in the VANET cluster. This new security framework uses distance calculation to determine the location of the node with respect to its transmission range. Also, the location of the node transmitting its location to RTMU, undergoes the displacement calculation for that particular node. The distance and displacement are analyzed to find the abnormality in the movement. In case the abnormality is found, the node is marked as the prankster node and all other nodes in the cluster are informed about the prankster node. The node position calculation formula used in this simulation is given below:

$E = (Cx^2-Dx^2)- (Cy^2-Dy^2)$

If **$E<R^2$**, Node is within transmission range

If **$E==R^2$**, Node is almost on the outer boundary of transmission range

If **$E>R^2$**, Node is out of the transmission range

Where Cx and Cy are the coordinates of the VANET node being analyzed lets say **Node-X** and, Dx & Dy are the coordinates of RTMU. **R** represents the radius of the transmission range of RTMU. **E** represents the distance between the RTMU and the **Node-X.**

V. RESULT ANALYSIS

In the ordinary VANET scenario, where the VANET cluster is not able to mitigate the attacks on its own, the accidents happens which leads towards the traffic chaos. The following figures are showing the ordinary situations.

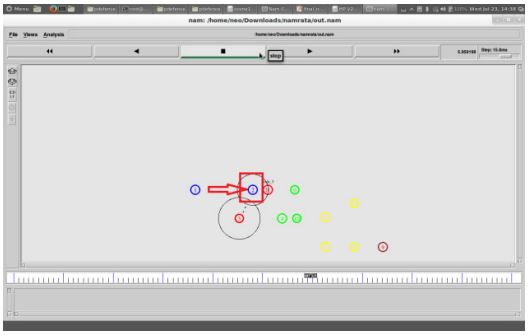

Fig. 1. The movement node 2 is interfered by node 3 using false information about its position.

The VANET is not capable of understanding or mitigating the prankster attack, which led to the collision between two nodes of VANET cluster. Whereas, in the proposed scenario, an road side traffic management unit (RTMU) has been used. The nodes in the VANETs are location aware and can propagate their location to the RTMU. RTMU performs various mathematical computations with respect to the size of the VANET cluster based on the transmission range of RTMU.

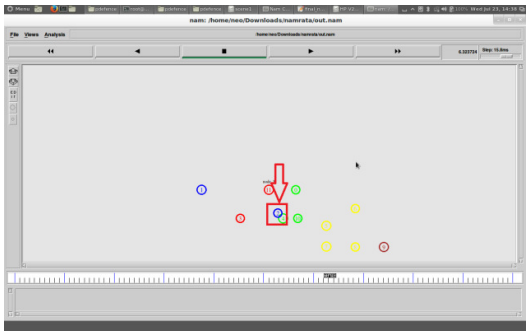

Fig. 2. Node 2 takes a precautionary path and the collision occurred between node 2 and node 4.

The RTMU computes the distance between the moving vehicle nodes within the cluster and scan the cluster movements for abnormalities. Whenever if locate the abnormality, it rectifies the problem and update all of the nodes in the VANET cluster. The nodes ignore the prank node and run over the fake location coordinates, which prevents the traffic congestion and facilitate the smooth traffic movement within the VANET cluster.

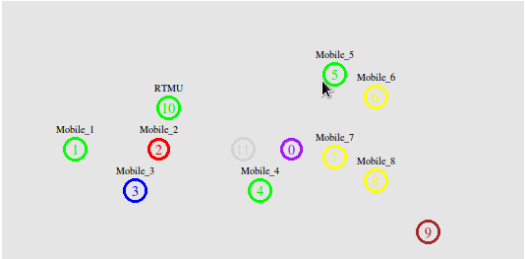

Fig. 3. The node 2 is being observer by RTMU as victim node in the new scenario.

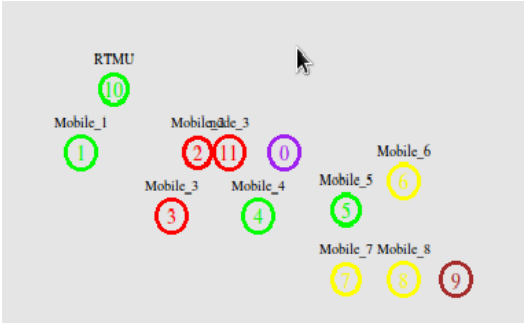

Fig. 4. The node 2 stopped itself after receiving smooth stop signal from RTMU because a node 11 suddenly appeared in front of it.

The node 2 has stopped after receiving the smooth stop signal from RTMU in this scenario because a node 11 suddenly appeared in its way. The node 11 is a prankster node propagated by node 3 in the cluster.

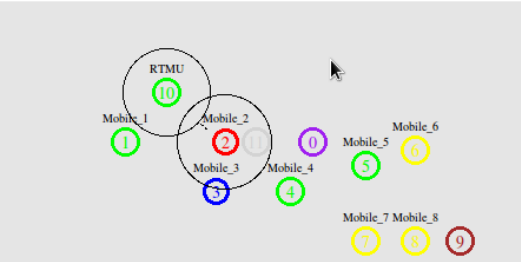

Fig. 5. The RTMU has rectified the problem and updated all nodes about the node 11and attacker node 3.

It is like a replica of node 3, where node 3 is pretending its new location with node 11. The RTMU has found the abnormality in the movement of the node 3 by analyzing its sudden displacement which is not possible in the case of automatically driven vehicles. The RTMU then rectifies the problem by declaring node 3 as prankster node, and node 11 as fake node created by the attacker.

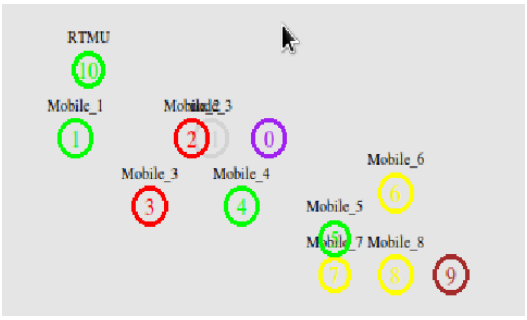

Fig. 6. Node 2 have started moving after receiving the start signal from RTMU.

This is how the threat has been mitigated by the RTMU.

VI. CONCLUSION

The proposed model has shown the effectiveness of working architecture of the new prankster attack mitigation framework. The new model has been successful in mitigating the prankster attack by detecting the prankster attack and finding the prank & the attacker nodes by analyzing the abnormalities in the vehicular ad hoc network cluster, which are found by calculating the distance between the cluster node and their individual displacements based on time slots.

The results obtained from the new prankster attack mitigation model have proved the effective application of the new model.

This model can be enhanced for other similar attacks like Sybil attack. The existing model can be improved to mitigate multiple prankster node locations propagated by a single or multiple hackers.

REFERENCES

[1]. Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin (2013). "Security and Privacy Enhancement in VANETs using Mobility Pattern" *(IEEE, 2013).*

[2]. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures (2010). "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" (IEEE, 2010).

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

[4]. Muhammad A. Javed and Jamil Y. Khan (2010). "A Geocasting Technique in an IEEE 802.11p based Vehicular Ad hoc Network for Road Traffic Management".

[5]. Chia-Chen Hung, Hope Chan, and Eric Hsiao-Kuang Wu (2008). "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks" (IEEE WCNC 2008).

[6]. João A. Dias, João N. Isento, Vasco N. G. J. Soares, Farid Farahmand, and Joel J. P. C. Rodrigues *"Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" (2011 IEEE).*

[7]. Steffen Moser, Simon Eckert and Frank Slomka (2012). "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks" 2012 IEEE.

[8]. Irshad Ahmed Sumra, Halabi Hasbullah, J. Ab Manan Mohsan Iftikhar, Iftikhar Ahmad, Mohammed Y Aalsalem (2011). "Trust Levels in Peer-to-Peer (P2P) Vehicular Network" 2011 IEEE**.**

[9]. Irshad Ahmed Sumra, Halabi Hasbullah, Jamalul-lail Ab Manan, (2011). "VANET Security Research and Development Ecosystem", 2011 IEEE.

[10]. Lu Chen, Hongbo Tang, Junfei Wang, (2013). "Analysis of VANET Security Based on Routing Protocol Information", 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China pp.134-138.

[11]. M. Khabazian, M.K. Mehmet Ali, (2007). "A Performance Modeling of Vehicular Ad Hoc Networks (VANETs)", 2007 IEEE.

[12]. Yi Qian, Kejie Lu, and Nader Moayeri (2008). "Performance Evaluation Of A Secure Mac Protocol For Vehicular Networks" (2008 IEEE)**.**