Protection Against DDOS Using Secure Code Propagation In The VANETs

Mandeep Kaur, Manish Mahajan

Mandeepcheema6@gmail.com,cgccoe.hodcse@gmail.com

ABSTRACT--VANETs are the vehicular networks used to connect the vehicles together to share their information with each other in the cluster. The hackers are used to attack VANETs with various means of attacks. Many security techniques are used to mitigate the risks caused by the attacks to cause ill-effects to 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 DDoS attack by using road side traffic management unit (RTMU). The RTMU is using various mathematical computations for traffic pattern analysis to detect the abnormality in data traffic between the cluster nodes. All of the nodes in the scenario are GPS location aware nodes and sharing their location actively with RTMU. Also all of the VANET nodes communicate with each other through RTMU. The results have shown the effectiveness of the proposed model to mitigate the DDoS attack and facilitate smooth traffic movement.

KEYWORDS: *VANET security, DDoS, Road side unit, network traffic analysis, and VANET resource unavailability attacks*

INTRODUCTION

Vehicular ad hoc network (VANET) is consisting of the nodes which are the vehicles (moving cars) is a subclass of the MANET's (Mobile ad hoc network). The VANET infrastructure is varying according to the range of the network. Any node which comes within the range can be a part of the network. When the car moves out of the range, they leave the network. It may consist of the large no. Of the nodes (vehicles) which require some authority to govern it. The RSMU (road side management unit) used to connect the vehicles which are moving on the road and to other network devices. Every vehicle has an OBU (On board

unit), which are capable of connecting the vehicles with the RSMU through the DSRC radios. The TPD stands for the Tamper Proof Device, it contain the information such as the driver's identity, speed, route, trip detail etc.

DSRC stands for the dedicated short range communication it occurs when the vehicles use the radio signal to communicate with one another. VANET system spread the emergency and traffic information among the vehicles in a timely manner. It is the ad hoc communication in which no wires are required, all the nodes can move freely. VANET networks are ad hoc network in which mobile nodes uses the wireless communication to communicate one another. Vehicular network is also known as the intelligent transportation system in which the two types of the communication may be occurring: 1) vehicle to vehicle communication (V2V) and 2) vehicle to road side communication (V2R) in which the roadside unit broadcast the messages to all other vehicles it is also known as the single hop broadcast. It provides the high bandwidth link between the road-side unit and the vehicles [1].

The protocols that are used in the VANET network are the ad hoc routing protocols; they are also implemented for the MANET's. Mostly, the VANET network uses the address based and topology based routing protocols. The characteristics of the VANET network are high dynamic topology (choice of the path and speed defines the dynamic topology and the frequent disconnected network and hard delay constraints. The network scalability, securing mobility (vehicles in a VANET have a high degree of mobility), volatility (the same connection among the vehicles will not happen again) are some of the challenges against the VANET network. One of the challenges that are facing by the ad hoc networks are the highly change in the topology.

There are the no. The threats in the VANET environment such as denial of service attack (DOS), distributed denial of service attack (DDOS), Sybil attack, alteration attack, black hole attack, fabrication attack, reply attack etc. DOS attack can be performed by the insider and outsider of the network [4][5]. In the DDOS attack, the attack is launched on the node from the different locations in a distributed manner so that the node can- not communicate with other nodes (vehicles).

The goal of the VANET system is to build a vehicular communication system to provide the data more quickly for the benefit for the passenger ease, comfort, and safety. The VANET applications are divided into safety and non-safety applications. Safety applications are concern with the human life where as the non-safety applications pleasant with the passengers. [1][3] Examples include travelling map, outdoor car parking etc. For the future road traffic management system the VANET network becomes the necessary component. The reason behind to develop this network is to improve the security, efficiency, safety of the vehicles. One of the advantages of VANET system is that the cost of maintenance and implementation is very low.

LITERATURE REVIEW

Ghaleb F. and his associates 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 G. 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.p has proposed an effective security mechanism for ill-defined problem in VANETs. Qian.yi 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 geo-casting based protocol based IEEE 802.11p 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 P2P VANETs.

PROBLEM FORMULATION

In the given scenario in the base paper, the solution against denial of service attack for VANETs is proposed and implemented. The solution is implemented on each node independently so that all nodes can become capable of mitigating the denial of service attacks on their own. But the denial of service attack is not very efficient in making the service available. So, the hackers use distributed denial of service attack instead. We have taken one another paper into account for the security against denial of service attacks. This paper uses self-adaptive decentralized solution (SAD) against selective jamming attack (A form of DOS attack) for WSNs. Both of the algorithms work with pattern recognition and then mitigate the attack by blocking the packets coming from the compromised origin. Distributed denial of service is the most dangerous attack and has proved to be more effective than denial of service because it is launched by multiple nodes together. Botnets or individual nodes can be used to launch a DDoS attack. The existing techniques in both of the papers are not capable of protecting against selective jamming, in order to address multiple nodes attempting to join the network at the same time i.e. Distributed Denial of Service (DDoS) attack. The existing protocol can be improved to protect against selective jamming attack in order to multiple nodes, a specific and severe DDoS attack.

PROPOSED RESEARCH MODEL

In the research project, we propose an effective improvement in the existing method to make it capable of protecting the VANETs against DDoS attacks. The new solution will work on the individual nodes and will make each VANET node capable of mitigating DDoS attack on its own by analyzing the abnormalities in the traffic patterns. This protocol will generate multiple random unique codes and add them to the inter communication packets, at the sender's side. On the receiver side, these unique codes will be verified using the unique code verification calculation method. This will protect the nodes by discarding the non-matching packets from external nodes attempting to launch DDoS on VANETs.

METHODOLOGY

At first stage, a detailed literature study would be conducted on the denial of service or distributed denial of service attacks and solution for VANETs. Literature study will lead us towards refining the structure of the proposed security solution design. Afterwards, the proposed solution will be implemented in NS2 simulator and a thorough performance analysis would be performed. Obtained results would be analyzed and compared with the existing techniques. The detailed literature survey has been conducted on resource unavailability attacks and their defense mechanisms. The prototype of the base paper has been implemented in the NS-2 simulator. The performance analysis has been performed on the base paper implementation. In the future, the proposed system will be developed using NS2 & the comparative analysis between existing system v/s proposed system will be performed.

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 DDoS attack by detecting the attacking packet streams by analyzing the abnormalities in them for the smoother movement in the vehicular ad hoc network cluster, which are found by analyzing the packet streams. 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 attacks like Sybil attack or prankster attack. The existing model can be improved to mitigate multiple attacking nodes at a single slot of time.

FUTURE WORK

In future, the new security mechanisms against DDoS, black hole or other variant of DDoS (like selective jamming attack, packet dropping attack, etc.) AODV or TORA can propose. Also, the best considered AODV protocol can be compared with the other candidate protocols used for VANET simulations. AODV or TORA, or both of them can be compared with more protocols or with each other under different conditions in VANETs or other environments.

REFERENCES

[1] S. RoselinMary, M. Maheshwari, "Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)", vol. 1, issue 1, IEEE, 2013.

[2] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, "SAD-SJ: a

Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 1, pp. 1-8, IEEE, 2013.

[3] Constantinos Kolias, Georgios Kambourakis, Stefanos Gritzalis, "Attacks and Countermeasures on 802.16: Analysis and Assessment", CST, vol. 1, pp. 487-514, IEEE, 2013.

[4] Md. Monzur Morshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 1, pp. 571-576, IEEE, 2013.

[5] Sonali Swetapadma Sahu, Manjusha Pandey, "Distributed Denial of Service Attacks: A Review", vol. 1, pp. 65-71, IJMECS, 2013.

[6] Ms. Poonam Barua, Mr. Sanjeev Indora, "Overview of Security Threats in WSN", vol. 2, issue 7, pp. 422-426, IJCSMC, 2013.

[7] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", ITMC, vol. 12, issue 2, pp. 318-332, IEEE, 2013