# A Novel Security Approach for Data Flow And Data Pattern Analysis To Mitigate DDOS Attacks In VANETs

Mandeep Kaur, Manish Mahajan
Mandeepcheema6@gmail.com, cgccoe.hodcse@gmail.com

*ABSTRACT*—The VANET security is an important issue with the rise of the automatically driven vehicle based technologies. The automatically driven vehicle based clusters are programmed for each vehicle to run individually by coordinating with all of the other nodes in the VANET cluster. The proposed model has been designed to detect and mitigate the DoS and DDoS attacks in the VANET clusters to avoid any of the misbehavior or mis-happening in the form of VANET node failure, collision or in any other form. The DDoS attack prevention algorithm works as the real time attack detection and overhead data filtering algorithm in order to protect against the DoS and DDoS attacks. The proposed model result has been obtained on the basis of network load, throughput, packet delivery ratio, etc. The experimental results have proved the efficiency of the proposed model in comparison with the existing models.

*Keywords*—VANET security, Denial of service, distributed denial of service, resource unavailability attacks.

## INTRODUCTION

VANET (vehicular ad hoc network) are very favorable mechanism to enhance the traffic safety and capability. It also facilitates or authorizes the other number of applications in the domain of vehicular communication. The applications which are proposed for the VANET have various properties and need non-standard communication protocols. The changes of the network because of the vehicular node movement again confuse or complicate the suitable communication system. The communication pattern and data flow analysis deepen the understanding of the VANETs. It also makes easy the development of the VANET communication system. [3]

Vehicular networks and vehicular ad hoc network has been broaden to a huge number of different applications that can benefit from wireless communication among the vehicular nodes [3][4]. These days, vehicles not only conceived to communication among each other but also gain the information from and transmit data to infrastructure units. Stationary chunk of the vehicular ad hoc network vary from traffic lights. The different traffic signs helpful to access points at gas stations, home and in another place. The active safety applications show the traffic efficiency applications, the central idea, entertainment applications and business applications. Active safety applications taken as a typical and desirable group of applications for the vehicular network which have the direct effect on the safety of the road [6].

The applications which are based on the vehicular communication vary from simple transfer of vehicle status data to huge complicated large scale traffic management contain infrastructure integration. The emergency vehicles may be capable to reach their destination more quickly than today. Vehicular network attempts to support the public service like emergency recovery units or police.

Data flow analysis is a mechanism to collecting the data or knowledge about the attainable set of values computed at different points in a comp. Program. Program's CFG (control flow graph is used to identify the element of a program to which a specific value appoint to the variable might

inseminate. When optimizing a program, the data or knowledge collected is used by the compiler. A legal example of the data flow analysis is reaching definitions. An easy method to carry out the data flow analysis of a program is to build up data flow equations for every node of the CFG (control flow graph). Resolve these equations by frequently computing the output from the given input at every node till than the complete system becomes secure.

Data flow analysis can be done in a different ways such as forward analysis and backward analysis. Few data flow problems need backward flow analysis. It pursues the same plan rather than the transfer function is applied to exit state not to the entry state where as the join operation applied to the entry states. Every type of the data flow analysis has a particular transfer function and joins operation. In the forward flow analysis, the entry point plays a vital role. Its entry state is right defined at the beginning of the analysis. For some cases, the local variables with known values are blank. If there is no cycle in the control flow graph (CFG) then the equations are solving directly. Then the control flow graph can be topologically sorted. At the beginning of every block, the entry states can be calculated.

Increasing or expanding the Traffic pattern analysis and traffic measurement is more and more vital. The incrementally usage in the wired network may lead to the constraints. The DDOS attack sources have a form of the pattern behaviour to transmit the packets. It is an effective approach to predict the known pattern for discovering. In the mobile networks usage of the high speed packet data services has grown from 10% of the complete traffic of the mobile network in sep. 2006 to 75% in July 2008. The highly internet access availability with similar to wired capacity in the mobile networks also arises the question how the radio network will manage the traffic demands of user. In route planning and to avoid the traffic jam the information about the traffic conditions on the road plays a vital role.

Due to the development of the technology, it becomes feasible for the vehicular nodes to furnish with the communication and GPS system. Equipped nodes are used to gather the information about traffic conditions like speed, position and direction from the vehicular nodes. Based on the number of node that joining the ad hoc network, this gathered data can impart the useful knowledge about the driving conditions. This information with the proper analysis can be used to discover and imagine the traffic jam conditions [1]. The information collected about the traffic by a vehicular node in the ad hoc network is scene as a snapshot in time of the current traffic conditions. The snapshot is taken as a pattern and it is analyzed by using a different pattern analysis techniques. The benefaction of this paper is listed below:

- Feasibility: Our traffic pattern detection method could be capable to implement in real world cased depending on the internet technology. Due to the low complexity and light calculation the detection methods are possible to implement with other network equipments like hub, switch etc.
- Real-time implementation: Our detection methods are capable to discover the DDOS attacks in a little period of time.
- Flexibility: This detection method could be capable to discover the attack packets like TCP, UDP, application-based floods etc.

## LITERATURE SURVEY

S. RoselinMary et al. [3] have suggested an “Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)”. In this paper, the authors have presented an Attacked Packet Detection Algorithm (APDA) that are used to find out the DOS (Denial-of-Service) attacks before the verification time. This decreases the overhead delay for processing and improves the security in VANET.

Marco Tiloca et Al. [4] have proposed a "Wireless Sensor Networks (WSNs) are used in the number of application scenarios, like industrial applications and factory automation. Typically, Time Division Multiple Access (TDMA) is used for data communication among sensor nodes. Still, TDMA-based WSNs are particularly liable to Selective Jamming attack. It is a kind of the Denial of Service (DOS) attack aimed at severely hindering the network reliability. The author presented the SAD-SJ, a self-adaptive and decentralized MAC-layer solution towards selective jamming in TDMA-based WSNs. SAD-SJ does not need a central entity, require sensor nodes to depend only on local information, and grant them to join and leave the network without stopping other nodes activity.

Morshed et Al. [12] have proposed, "Cluster Based Secure Routing Protocol (CBSRP) is a MANET routing protocol that guarantees secure key management and communication among mobile nodes. It uses Digital Signature and one Way hashing technique for safe communication. According to CBSRP, it builds a group of small clusters made up of 4-5 nodes and after that the communication occurs among mobile nodes. Inner a cluster, there is ever a cluster node or cluster head. The cluster head inner the cluster is not constant as other nodes hold in the queue and depend on the priority new cluster node or cluster head is choosen from rest of the node. Inner a cluster, mobile nodes are authenticated using one Way Hashing concept and Digital Signature is not urgent for cluster communication.

Thapngam, Theerasak, et al. [1] have proposed a behavior based detection that can prejudice Distributed Denial of Service (DDoS) attack from authenticated traffic unconcerned to different types of attack packets. Current DDOS attack is brought by the worms, attack tools etc. we observe that the DDOS attack have the characteristics of repeatable patterns which are distinctive from authenticate flash crowd traffics.

## ALGORITHM OVERVIEW

In this paper, we have developed a new security framework to mitigate the DDoS attack in the VANET cluster. This new security framework uses packet and location analysis to determine the attacker node and in order to block the data generated from the attacker node. In case the abnormality is found in the data transmitted by attacker node, the node is marked as the DDoS node and all other nodes in the cluster are informed about the attacker node and stop receiving the data from that node.

The fixed nodes will communicate with each other in the cluster. Assume that fixed nodes A, B and C are located from west to east respectively. So if a vehicle will enter in the coverage of fixed node A to fixed node B, it is detectable that vehicle is moving into the similar direction. The attacker nodes would be examined by the intermediate node (RTMU or RSU in this scenario). So our method will be able to detect the attacking and normal packet streams by analyzing the data sent from the attacker node. Hence, a vehicle will not be able to propagate the attacking packet streams in the VANET cluster.

Algorithm 1: proposed system

1. Node X1 and X2 send a neighbor request to node X.
2. Node X examines the location of node X1 and X2, and permit them to join the VANET cluster.
3. Node X examines the packet stream, its size and payload information.
4. If packet size remains same for every packet, it examines the payload information. If payload information is found same in two packet of a single communication stream, it is marked as possible attacker.
5. If the number of same packets increase a certain limit, the sender node is marked as the DDoS attacker and the information is provided to all of the nodes in the cluster.

6. All nodes block the attacker node and stop receiving the packets from the attacker node.

## RESULT ANALYSIS: Simulation results of VANET with security implemented

The VANET simulation has been implemented under the influence of AODV routing protocol in the controlled simulation scenario. The ad-hoc on-demand distance vector routing protocol (AODV) is best capable of providing the routing services to the moving stations. The simulation scenario has been implemented with almost 15 nodes. In the simulation scenario, the nodes can be described as the base stations (which are being used as the road side units, RSUs), victim node, attacker nodes and the normal nodes. Out of the all VANET nodes the four major categories can be defined on the basis of their communication link role such as sender nodes, receiver nodes, end routing nodes or
traversing nodes. In this simulation, there is one victim node and five attacker nodes in the VANET scenario of DFDPA is being implemented and tested thoroughly. The results has been obtained from the victim node in order to analyze the performance of the victim node under the given attack situations. The results have been obtained in the form of network load and transmission delay under the given simulation conditions. The performance metrics chosen for the evaluation of Distributed Denial of Service attack are end-to-end delay, throughput and network load. Following important performance :

End-to-End Delay -- The end-to-end delay is the time from the generation of a packet by the source up to the destination reception, so this is the time that a packet takes to go across the network. This time is expressed in seconds (sec).

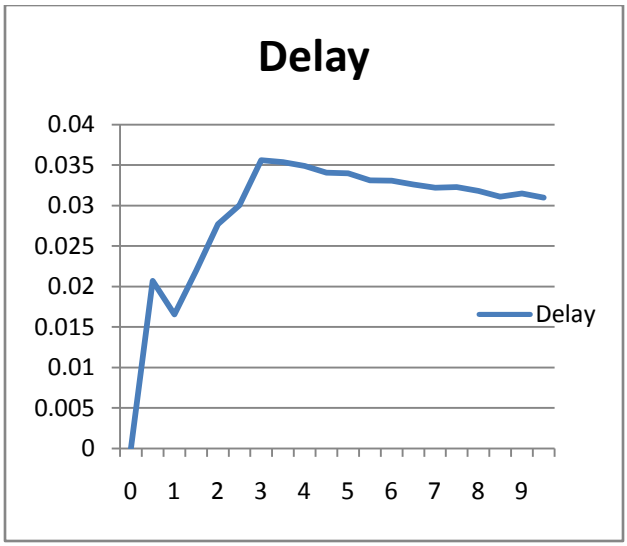



Figure 1: The graph transmission delay is represented from the testbed simulation for the proposed model testing.

In the proposed simulation, the proposed model has been designed to add the betterment in the results of the proposed model algorithm in case of the flooding attack in the form of distributed denial of service. The proposed model has been recorded nearly at 0.035 seconds of delay at the maximum level. The delay of 0.035 seconds can be considered extremely low in the wake of the performance improvement in the existing model. The proposed model has been proved to be significantly well in the terms of data delivery efficiency in the VANET nodes. The minimum delay has been recorded at zero and maximum at 0.04 seconds approximately which shows the vigorous performance of the proposed model. The proposed model has been recorded with the average delay of approximately 0.03 throughout the simulation.

Throughput -- Throughput or Network throughput is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the

receiver to receive the last packet. It is represented in bytes per second or packets per seconds.

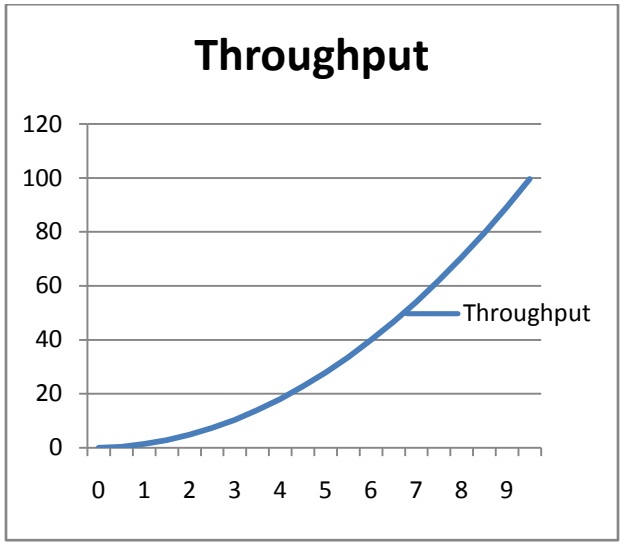
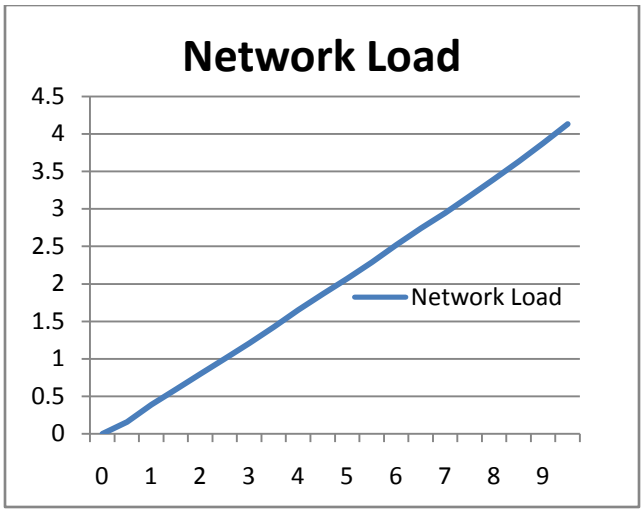



Figure 2: Throughput is represented in above figure

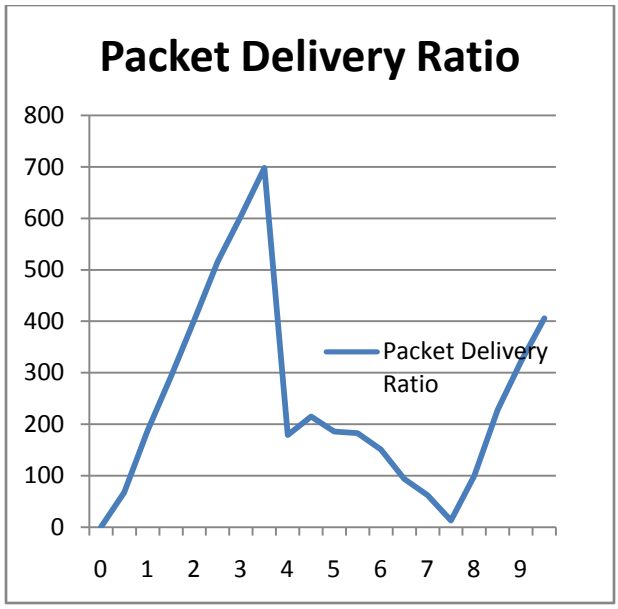
Throughput has been shown under the secure VANET over AODV protocol shown in the figure 2. The throughput has been recorded significantly higher than the existing models in the approximately similar situations. The throughput has been recorded on the average value of almost 50 Mbps in the VANET cluster during the attack hours. The higher throughput indicates the successful mitigation of the attack over the nodes undergoing the attack situations from the multiple attacker nodes.

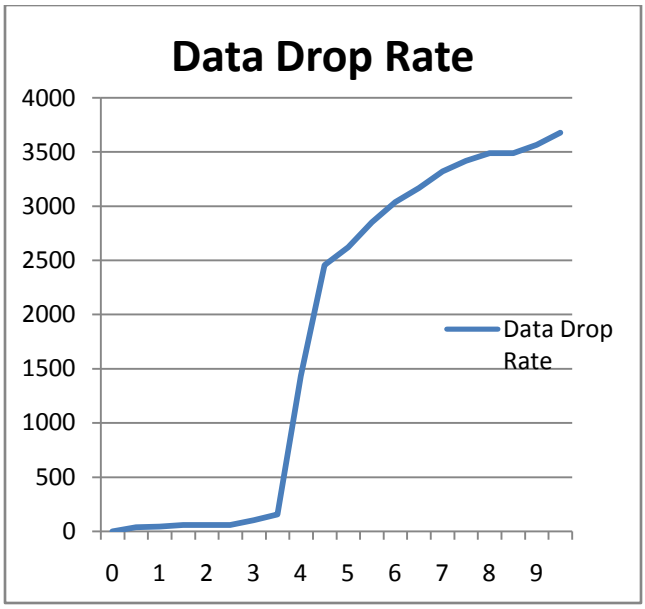
Network Load -- Network Load is the amount of data (traffic) being carried by the network at a particular time. The network load varies from time to time. It is represented in bytes per second or packets per seconds**.**




The maximum network load of under 4.5 Kbps indicates the better performance of the VANET cluster under the DDoS attack situation. The DDoS attack has been launched from the multiple users within the cluster, which has not affected the load of the VANET cluster, which shows the greater performance of the proposed model in tackling the DDoS attack.

Packet Delivery Ratio -- Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets generated or sent from the source. It describes the loss rate. The Performance is better when packet delivery ratio is high.




The packet delivery ratio is the most variable ratio among the all parameters fetched during the proposed model results evaluation. The packet delivery ratio depends upon the traffic rate and the reliability of the links between the VANET nodes. The lowering packet delivery ratio in the later stages was due to the DDoS attack over the VANETs, which is later solved up and the attacks is mitigated successfully.

Data Drop Rate: The data drop rate is the parameter which indicates the performance of the proposed model in the form of data loss due to the link bottlenecks or due to traffic overflow or other similar or non-similar reasons.

The data drop rate has been studied in the rising pattern while studying the performance evaluation of the proposed model under the DDoS attack simulation. The maximum drop rate of 4000 bytes has been recorded during the complete simulation out of the millions of bytes being transmitted across the given links in the VANETs.

## 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 the future, the proposed security mechanism can be integrated with other security mechanisms to reduce the impact of DDoS attack from the VANET networks. The effective attack mitigation mechanisms can avail the maximum uninterrupted movement in the VANET clusters. Also, the proposed model can be enhanced by improving the working of the proposed model.

## REFERENCES

[1] Thapngam, Theerasak, et al. "Distributed Denial of Service (DDoS) detection by traffic pattern analysis." *Peer-to-peer networking and applications* 7.4 (2014): 346-358.

[2] Ghosh,M.,Varghese,A.,Kherani,A.A.,Gupta,A.: Distributed misbehavior detection inVANETs.In:Wireless Communications and Networking Conference,WCNC IEEE, pp. 1–6 (2009)

[3] RoselinMary, S., M. Maheshwari, and M. Thamaraiselvan. "Early detection of dos attacks in VANET using attacked packet detection algorithm (apda)."*Information Communication and Embedded Systems (ICICES), 2013 International Conference on*. IEEE, 2013.

[4] Tiloca, Marco, et al. "SAD-SJ: A self-adaptive decentralized solution against Selective Jamming attack in Wireless Sensor Networks." *Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on*. IEEE, 2013.

[5] Kim, C.H., Bae, I.H.: A misbehavior based reputation management system for VANETS.LNEE 181, 441–450 (2012)

[6] Daeinabi, A., Rahbar, A.G.: Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. Multimedia Tools Appl. 66(2), 325–338 (2013)

[7] Wahab, O.A., Otrok, H., Mourad, A.: A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles. Comput. Commun. 41, 43–54 (2014). Elsevier

[8] Vulimiri, A., Gupta, A., Roy, P., Muthaiah, S.N., Kherani, A.A.: Application of secondary information for misbehavior detection in VANETs. IFIP. LNCS, vol. 6091, pp. 385–396. Springer, Berlin (2010)

[9] Douligeris C, Mitrokotsa A (2004) DDoS attacks and defense mechanisms: Classification and state of the art. Comput Netw 44(5):643–666.

[10] Peng T, Leckie C and Ramamohanarao K (2007) “Survey of network-based defense mechanisms countering the DoS and DDoS problems.” In: ACM Computing Surveys, Vol. 39, No. 1, April 2007.

[11] T. Bonnedahl: Traffic Measurement and Analysis in Fixed and Mobile Broadband Access Networks, Dept. of Electrical and Information Technology, Lund University, Master Thesis, 2009

[12] Ghosh, M., Varghese, A., Gupta, A., Kherani, A.A., Muthaiah, S.N.: Detecting misbehaviors in VANET with integrated root-cause analysis. Ad Hoc Netw. 8, 778–790 (2010)

[13] Morshed, Md Monzur, and Md Rafiqul Islam. "CBSRP: Cluster Based Secure Routing Protocol." *Advance Computing Conference (IACC), 201S3 IEEE ss3rd International*. IEEE, 2013.