ISSN (e): 2250 – 3005 || Volume, 09 || Issue, 5 || May– 2019 ||
International Journal of Computational Engineering Research (IJCER)

Improving Throughput, Analysis of Throughput under Eavesdropping and DDOS Attacks for DADCQ Protocol in VANET

Dharmaveer P. Choudhari1, Dr.S.S.Dorle2
1 PhD Research Scholar, Department of Electronics Engineering, G.H.R.C.E, Nagpur, India
2 Professor Department of Electronics Engineering, G.H.R.C.E, Nagpur, India
Corresponding Author: Dharmaveer P. Choudhari

ABSTRACT: *In recent period of time there is a tremendous growth in the wireless technology due to the advancements in technology. And because of the advancement of the technology it has made possible to design and develop the various types of network in the different environments. The most important thing is that VANET has become a growing for the researchers to have the research on the various issues such as driver and passengers' safety, reduce congestion of traffic. So the VANET is the very vast area where the research is still going to provide road safety from all perspectives.*

Keywords: *DADCQ, Throughput, VANET, Eavesdropping.*

Date of Submission: 07-05-2019 Date of acceptance:24-05-2019

I. INTRODUCTION:

As seen from the last decade the mobile communication has given a tremendous transformation of mobile communication techniques to the vehicular industry and which is a very great achievement from the safety of vehicles. This allows the various vehicles to communicate with each other in the feasible manner and to communicate within themselves. This advancement allows the driver to share the valuable information with the adjacent vehicles in the data range. This valuable information may be about any danger in the upcoming pathway of the vehicles or any kind of the emergency service required by the vehicles. So for such kind of scenarios VANET plays a very key role for providing the safety to the diver's in the dense network such transmitting safety alert messages to all the vehicles in the network so that all the vehicles can read the message and can take the necessary action. Now VANET has opened the door of the various safety precautions that can be given to the driver.

In VANET there are various mobile nodes the example of these nodes may be cars moving in the road which communicate with each other in the ad-hoc manner and forms the ad-hoc network. The data range of VANET is approximately about 100 to 300 meters. If the car goes out of the range then it will lose the network and no communication will be possible with the other cars in the network. And if the car comes in the range it can rejoin the network and communicate with other cars present in the network. Another application of VANET is that it is been deployed by the police and fire vehicles so as to communicate with each other in case of any urgent services needed. Also various automotive companies such as Ford, BWM etc. are also deploying the VANET. The multi-hop protocols are classified into two categories such as topological protocol and statistical protocol. The statistical protocol is the best suited for the VANET applications as these protocols are have the tolerance to the rapid changes that are occurring in the network topology and these protocols can be capable to make the transmissions resisting the fading and the collision present in the network.

In VANET there exists a dynamic topology as there is continuous change in the direction or the speed of the vehicles. Also the connectivity between the two nodes changes rapidly. There is unlimited storage capacity in the network which allows the various nodes to communicate with each other with the valuable information through the network. We have done the communication with the DADCQ protocol and all the network simulations have been done on the Network Simulator NS-2. The key feature of the DADCQ protocol is that it uses the distance method for selection of forwarding the nodes. This distance greatly depends upon the threshold function which is being designed in such a way so as to give the maximum reach ability for the VANET. About the threshold method it uses the common framework and the nodes uses the value of the variable and the location of the variable so as to calculate the threshold value for the protocol. And then decide whether to rebroadcast or not. As blindly retransmitting of the data can jam the network and thus can cause the broadcast storm problem in the whole network. So the value of the threshold function is very crucial to design for the DADCQ protocol. This distance method is particularly decided largely by the protocol parameter named as Dc.

Algorithm is simple is as following

a. Initialize D=1 if a message is received set d to the distance to sender D= min {D, d/r} so set a random back off timer.

b. If message is received during back off timer, repeat When the back off expires rebroadcast if D >Dc.

The process to any broadcast protocol that is the statistical one is the value of the decision cutoff threshold that is the value of Dc. If the value of the Dc is set too high value then the reach ability of the network may be degraded to the larger of its extent. And if the value of Dc is set too low value then the DADCQ protocol will not be able to prevent many nodes from the process of the rebroadcasting ultimately it will lead to broadcast storm problem in the network. So there is range of values selected for the decision cutoff threshold Dc. If this Dc is less than the minimum required critical value required for the DADCQ protocol then the reach ability is almost unity in all simulation scenarios. Near the critical value reach ability quickly jumps from one to zero which gives the indication that the reach ability is of highly variable nature for the protocol. If the node density is high then we can adjust the value of D_C to a more value to eliminate the surplus of transmissions. So D_C should be the function of local node density N that is the number of nodes present in the region that can be termed as the local node density. For this we need to find the minimum value of D_C at the many values of the global density which is termed as ‘λ’. This value of optimal value is the value for which the reach ability remains satisfactory. Then we must plot the optimal values and we need to find the suitable estimate function D_C (λ).Then substitute the local node density for the global node density ‘λ’ to get the value of D_C (N).Now we should test the value of D_C (N) to get the acceptable reach ability of the network. So adjust the value of D_C as required for the network reach ability. As the density of the node increases the value of the threshold becomes more powerful to prevent the unwanted rebroadcasts in the network. So the general form of the threshold function is as defined

$D_C (N) = D_{max} - \beta e^{\alpha N}$ …………………….. (1)

II. QUARDRAT-BASED THRESHOLD FUNCTION DESIGN.

In this section we will talk about the Quardrat-Based Threshold Function Design and we will include the spatial stastic ‘Q’ in our protocol so as to improve the protocol performance in the varying density of the network traffic. We will use the value Q so to calculate the value of the threshold function for the DADCQ protocol. The key point is that the value of the Q should be used in such a way that it should be well for the both 1D and 2D networks. The parameter ‘α’ needs to be varied based on the distribution of the node.If it is three in 1D networks then it should be one time in the 2D networks. The value of the Q for 1D networks follows the following equation:

$Q_{1D \approx 1 + 0.125 N}$ (2)

If we consider the 2D network then the value of $Q \approx 1$ and $\alpha \approx \alpha_{2D}$. So when the network is 1D then we have the $Q_{1D \approx 1 + 0.125 N}$

and whereas the $\alpha \approx \alpha_{2D}/3$.Our job is to map the values of Q linearly between the 1D and 2D value for the scenario.As it is not easy to generate the values of Q and so we have taken a linear from which is chosen to fill the gap between the 1D and 2D network for the simplicity. As so the formed equation is as given as

$$D_c (N, Q) = 0.90 - 1.2e^{-0.099}(2(Q-1) \quad + 1)^{-1} N \frac{}{0.125N} \qquad (3)$$

III. DDOS ATTACKS IN VANET.

The Distributed Denial of Service which is also called as DDoS attacks s basically it is very crucial to ensure DDoS protection in the network from the various kinds of attacks. As in today’s scenario the whole security of business is dependent on the internet. These DDoS attacks can be done with the help of simple web services and these are capable of controlling even the most stable servers of the network. Now these attacks prevent or stop the various services of the network and they pause the all operations of the network. The various methods of the DDoS attacks are as follows:

a) Volumetric Attacks:

In this type of attack the attacker node consumes all the bandwidth of the network and thus shut down all the operations of the network. Also these nodes send a large number of requests to the server at the same time so even the most stable server will go down .When all of such kind of attacker machines are directed to attack the single server so the volume of traffic overloads the server and thus causes server to go down.

b) Application Layer Attacks:

There are several layers that make the internet and each of these layers use different kinds of protocol to transmit the information. The final layer is the application layer which is the seventh one as per the sequence. This layer is one that

Deals with the HTTP communication and SMTP communication of the network for the web browsing and e-mail services of the network. These DDoS attacks mask the malicious activities as the real human behavior to predict also utilize all the resources of the network.

c) Protocol Attacks:

Now in this type of attack the attacker node directly attacks the protocol by sending a ping request by the fake IP addresses. And these send the request which the false one to the real server. And the server responds to such request waiting endlessly. So the unnecessary resources are acquired which in turn blocks the network.

IV. EAVESDROPPING ATTACKS IN VANET.

The Eavesdropping attack is also called as sniffing attack of the network. In this attack someone is trying to steal the data from the computers or the vehicles present in the network. That transmits the data over the Vehicular Ad-hoc Network which may be alert or the safety message of the network. Basically Eavesdropping is the unauthorized reading of the network data. Eavesdropping makes the advantage of unsecured network to steal transmit and received data. Now the attacks are not very easy to detect as they do not to create any abnormality in the function of the network operations.

V. THROUGHPUT WITHOUT AND WITHOUT DDOS AND EAVESDROPPING ATTACKS.

Throughput is basically defined as the amount of the task performed by the device within a specific period of time the throughput. So throughput is the measure of amount of work which is completed against the time consumed and it is used to measure the performance of the network. The idea behind the throughput was to estimate the performance of the task and productivity of network. This generally calculated in terms of the task per second. Generally the throughput is the rate at which the something is been processed. In case of the communication networks such as packet radio networks or Ethernet the throughput is defined as the success rate at which the message is been delivered over the communication channel across the network. The data passes through the certain network node in the network. And the measure of the unit of the throughput is in bits per second or bps or it may be data packets per second or per time slot.

If we talk about the system throughput it is the summation of all the data rates which are been delivered to the all nodes in the network. For the analysis of the throughput queuing theory is best situated for anlaysis.In the queuing theory the load of the network is denoted in terms of the packets per unit time and we call it as the arrival time defined as ‘λ’ and the drop packets in per unit time and is called as the departure rate and is denoted by ‘μ’ .Throughput is just similar to bandwidth consumption of the network. This throughput may be disturbed by the various factors such as end-user behavior, analog physical medium or power of the system components of the network. When we consider the various affecting factors of the protocol then we find that the useful data rate of the transmitted data is very low as compared to the maximum achievable throughput and in practice the useful part is usually considered as the goodput.

Researchers of the communication network area are usually very eager to know about the performance of the system for the communication network. If we consider the fact from the users point of view then is how effectively the data is been received to the particular device according to his or her need. Or which is the fastest device that will deliver the data per unit cost so the designers of the system are mainly interested in designing such a model which will be having the capable effective architecture for the system with good performance. The maximum throughput is just equal to the digital bandwidth capacity of the network.

Number of Communications	Normal Throughput	Throughput with Eavesdropping attacks	Throughput with Eavesdropping and DDos attacks	Throughput after removal of Eavesdropping and DDoS attacks
5	207.68	200.03	205.13	214.8
10	207.66	200.49	205.13	218.03
15	208.80	202.72	205.71	215.26
20	207.94	201.88	205.74	214.33
25	210.76	206.9	205.47	220.4
30	208.58	205.95	205.84	216.43

35	210.55	206.51	206.22	218.45
40	210.88	206.16	206.71	215.63
45	211.51	209.39	206.41	212.54
50	211.45	209.80	207.95	219.41

Table.1. Throughput under different network attacks.

As seen from the above table we have consider throughput for various attacks such as DDoS and Eavesdropping attacks. We have used NS-2 as the simulator for our analysis. The first column indicates the number of communication between the nodes present in the VANET network. The Second column indicates the values normal throughput that the throughput which is under the consideration of various attacks such as DDoS and Eavesdropping. The third column indicates the values of the throughput under consideration of only Eavesdropping attacks. The fourth column indicates the throughput under the consideration of DDoS attacks only and last which is the fifth column indicates the values of the throughput under removal of the Eavesdropping and DDoS attacks that the throughput is been made safe from Eavesdropping and DDoS attacks.

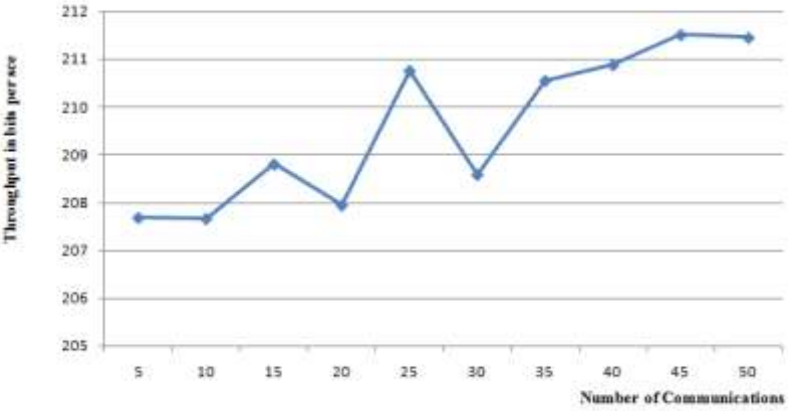

Fig. 1. Throughput under consideration of DDoS and Evaesdropping attacks.

As seen from the Fig.1. we have considered the throughput of the network under the consider of DDoS and Eavesdropping attacks so the values of the throughput is low due the attacks that are conserving the resources of the network so we are not getting the maximum value for the throughput that means the system has to be made free from the Eavesdropping and DDoS attacks.

Consider the Fig.2. Here we see the simulation results for the throughput by only consider the DDoS attacks of the network and we have masked the Eavesdropping attacks so only DDoS attacks are under the assumption so as the DDoS attacks are present in the system so there will be no effective proper communication and packets drop will be there and also loss of data will be there in the network which will cause the throughput to the lower value as seen from the simulation result of Fig.1. We have considered the sample of fifty communications.

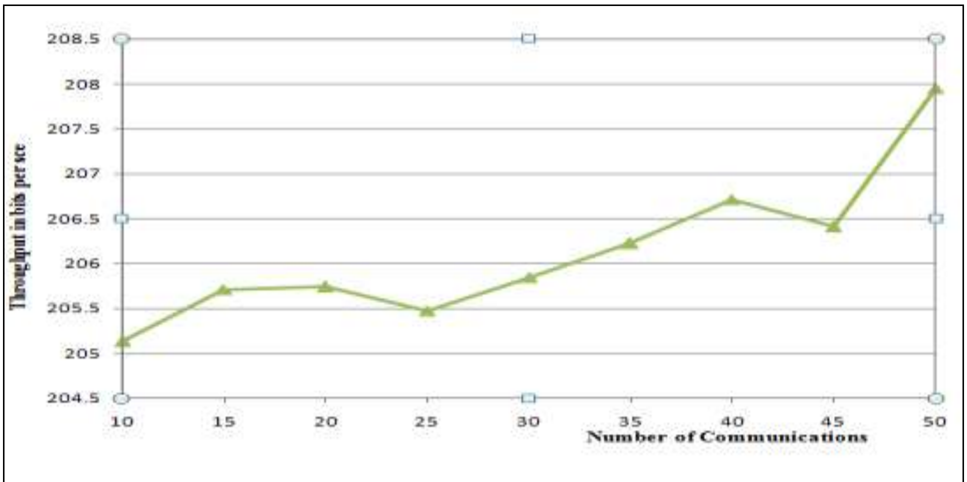

Fig.2. Throughput under consideration of DDoS attacks

As seen from the Fig.2. initially the throughput is low and it increases as the number of communication between the vehicles also increases so the value is not the maximum value of the throughput is achieved this is because the system is consisting of the DDoS attacks we are try to acquire the resources of the network thus making the network less efficient and thus decreasing the value of throughput making the system less efficient.

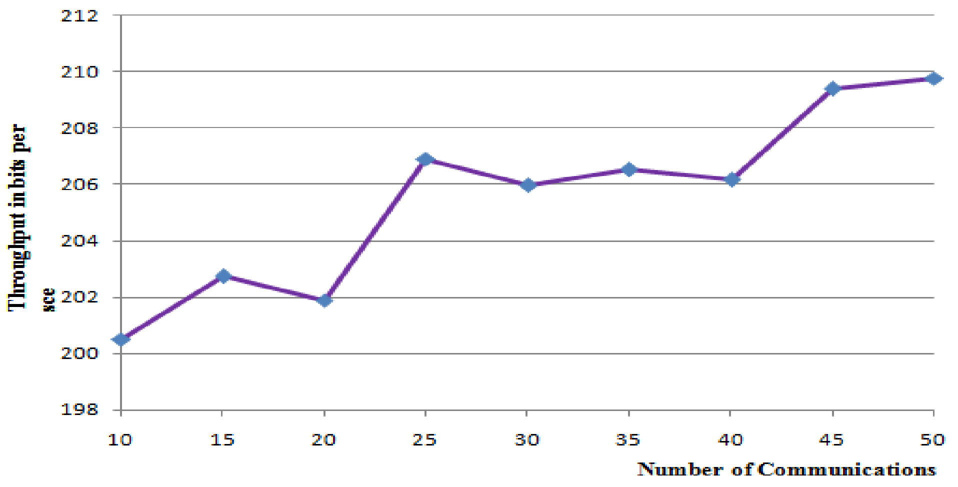

Fig.3. Throughput under consideration of Eavesdropping attacks

As shown in the Fig.3. we have considered the simulation results for the network only considering the Eavesdropping attacks and we have masked the DDoS attack for the network as we discussed earlier the Eavesdropping attacks are the attacks we are caused by the unauthorized reading of the data so this type of attacks causes the network to consume network resources thus utilizing the bandwidth of the network thus lower the efficiency of the network and which makes the network less efficient and makes the throughput to fall down to the lower value and reduced the data transmission over the network. Thus effective bandwidth of the network reduces.

As been analyzed the system under the various types of attacks such as DDoS and Eavesdropping we now will remove these two attacks and now we will see what is the effect of the removing attacks on the throughput of the network. As seen in the t Fig.4. We have shown the simulation results for the network after removing the DDoS and Eavesdropping attacks if we make the comparison with the three figures that is Fig.1. , Fig.2. & Fig.3.We can see that the throughput is very low due the presence of the DDoS and Eavesdropping attack so the value for throughput is low and we are getting the system which is less efficient in terms of throughput. And now if we consider the Fig.4. We can see that throughput value is quite high as we have removed the DDoS and Eavesdropping attacks so we a fair share of the bandwidth is available for the network and so data rate with the higher value is achieved and thus higher transmission is possible due to the removal of attacks.

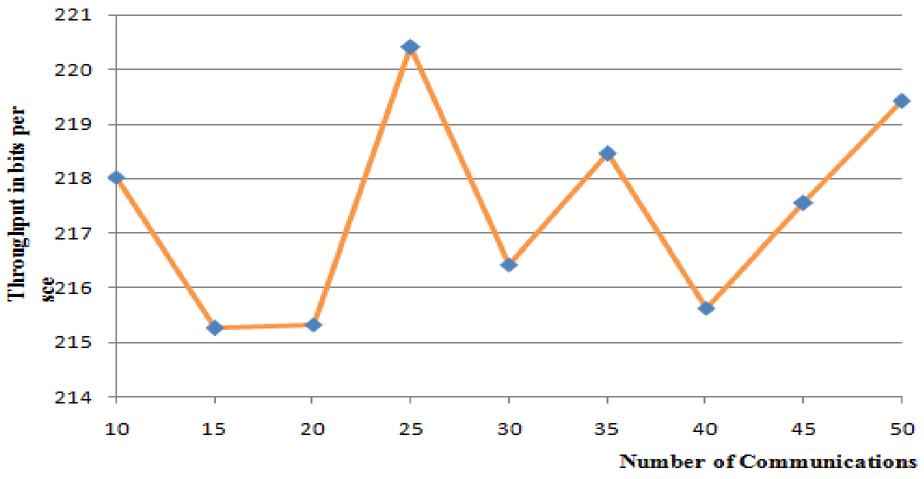

Fig.4. Throughput after removal of DDoS and Eavesdropping attacks

VI. CONCLUSION:

In this section we will discuss about the various conclusions we have got after the analysis of the above network. As seen from the Table .1. And Fig .1. , Fig .2. , Fig .3. Initially the effective value of throughput is quite low due the presence of the Eavesdropping and DDoS attacks so the bandwidth of the system is also low which gives rise to a lower quality of the network with packet drops and less bandwidth. If we consider the last column of the Table 1. We can see that we have achieved the higher value of the throughput as we have removed the attacks from the network from the Table .1. From the Fig .4. we can wee that higher value of the throughput is achieved to the previous three figures which itself proves the high throughput for the network. Hence we have higher value of throughput after removal of attacks.

REFERENCES

[1]. Michael Slavik, Imad Mahgoub,"Statistical Broadcast Protocol Design for Unreliable channels in Wireless Ad-hoc Networks" IEEE Globecom 2010 proceedings.

[2]. Michael Slavik, Imad Mahgoub,"Analysis of Beaconing Message Rate In VANET Multi-hop Broadcast Protocols." IEEE 2012.

[3]. YoHan Park,YoungHo Park,SangJae Moon, "ID-based Private Key Update Protocol with Anonymity for Mobile Ad-Hoc Networks" International Conference of Computational Science and Its Applications 2010.

[4]. SandeepTayal, MalayRanjan Tripathy"VANET-Challenges in selection of Vehicular Mobility Model".

[5]. Jan Janech ,Anton Lieskovsky, Emil Krsak,"Comparation of strategies for data replication in VANET environment" 26th International Conference on Advanced Information Networking and Applications Workshops, 2012 .

[6]. S.RoselinMary,M.Maheshwari, M.Thamaraiselvan,"Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)"

[7]. Fabio Leccese, "Remote-Control System of High Efficiency and Intelligent Street Lighting Using a ZigBee Network o f Devices and Sensors" IEE E TRAN SA CTIONS ON POWER D ELIVERY , VOL. 28, NO. 1, JA NUARY 2013.

[8]. Niko Vidgren, Keijo Haataja, Jose Luis Patino-Andres, Juan Jose Ramirez-Sanchis, Pekka Toivanen,"Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned" 46th Hawaii International Conference on System Sciences, 2013.

[9]. Mahmoud Hashem Eiza and Qiang Ni, Senior Member, IEEE"An Evolving Graph-Based Reliable Routing Scheme for VANETs", IEEE TR ANSAC TIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 4, MAY 2013.

[10]. Fang-Yie Leu, and Zhi-Yang LiDetecting DoS and DDoS Attacks by using an Intrusion Detection and Remote Prevention System" Fifth International Conference on Information Assurance and Security 2009.

[11]. Renato Preigschadt de Azevedo and Bruno Mozzaquatro and Alice Kozakevicius and Raul Ceretta Nunes,"DoS Attack Detection using a two dimensional Wavelet Transform" 2012 IEEE

[12]. FeiYe, RaymondYim, JianlinGuo, JinyunZhang and SumitRoy "Prioritized Broadcast Contention Control in VANET" IEEE ICC 2010 proceedings.

[13]. Nima Alam, Asghar Tabatabaei Balaei, and Andrew G. Dempster, Senior Member, IEEE "Relative Positioning Enhancement in VANETs: A Tight Integration Approach", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1MARCH 2013.

[14]. Michael Slavik, Student Member , IEEE, and Imad Mahgoub, Senior Member , IEEE, "Spatial Distribution and Channel Quality Adaptive Protocol f or Multihop Wireless Broadcast Routing in VANET",IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 4, APRIL 2013.

[15]. S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE communications Surveys & Tutorials, vol. 15, no. 4. pp. 2046–2069, 2013.

Dharmaveer P. Choudhari " Improving Throughput, Analysis of Throughput under Eavesdropping and DDOS Attacks for DADCQ Protocol in VANET" International Journal of Computational Engineering Research (IJCER), vol. 09, no. 5, 2019, pp 57-62