IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 2, Ser. II (Mar - Apr 2019), PP 44-47
www.iosrjournals.org

Eavesdropping Detection and Removal for Spatial Distribution and Channel Quality Adaptive Protocol in VANET

Dharmaveer P. Choudhari [1], Dr. S. S. Dorle, Ph.D. [2]
[1](*Research Scholar Department of Electronics Engineering, G.H.Raisoni College of Engineering, Nagpur, India)*
[2](*Professor Department of Electronics Engineering, G.H.Raisoni College of Engineering, Nagpur, India)*

Abstract: *Eavesdropping attack also known as sniffing attack in which someone is trying is steal the data that the vehicles or computers transmit over the vehicular adhoc network. Eavesdropping makes the advantage of unsecured network to steal the transmit and received data. Eavesdropping attacks are not easy to detect in the network as they do not create any abornarmality in the operation of the adhoc network.*
Keywords: *DADCQ, Global Predicator (GI), IOVs, Eavesdropper*

Date of Submission: 01-03-2019 Date of acceptance:18-03-2019

I. Introduction

Eavesdropping attack is a passive attack wireless network which is having the power to establish or forming a part of Internet of Vehicles (IOVs). In wireless communication encryption is the most commonly used method so as to protect the confidential data in the network. It is difficult to detect the eavesdropping attack in VANET due to various problems such as low capacity computational nodes, limited battery power, difficulty in managing the nodes in the centralized manner etchant so the countermeasures is to design a light weight vehicles, effective encryption algorithm for the transmitter and the receiver part[4]. The malicious nodes are also called as eavesdropper. If we detect the eavesdropper nodes we can know the activities of the eavesdropper nodes and find a good solution to protect the network. In this VANET the good nodes are mounted with the omi-directional antennas where as eavesdropper nodes are mounted by either directional antennas or omi-directional antenna[6]. Moreover the wireless network has more is having enormous interest from the both the industry and the academia.WNSs is being used in the environmental monitoring, surveillance security, farming so on.

Many studies assumed that senor nodes are being deployed in the random from an airplane. These scattered sensor network organize themselves to form ad hoc network in which the data packets are transmitted through multihops from the source node to the destination node, in WSNs any wireless node residing in the transmission range can potentially decode the signal both the transmitter and the receiver are unaware of the reconnaissance[9]. This reconnaissance is also known as eavesdropping activity has attracted the attentions.Morover specifically there are two types of eavesdropping attacks in WSNs

i)Passive Eavesdropping : In this the malicious node detect the information by listening the message transmission in the broadcasting wireless medium.

ii) Active Eavesdropping: In this the malicious nodes actively grab the information by sending quires on transmitter by misguiding themselves as friendly nodes. The study of the passive eavesdropping nodes is often more important than the active eavesdropper nodes.

Conventionally nodes consist of the omnidirectional antennas which are used to broadcast the signals uniformly in all the directions. In this transmission only a portion of the signal reaches and the most of signal is lost. And this property of radiating signals leads high interference. And both these two factors effects the performance of the wireless neteork.Compare to omnidirectional antennas the directional antennas can reduce the eavesdropping by concentrating the radio signal in the desired direction. So in the other undesired direction there are no radio signals. So therefore using the directional antennas can reduce the eavesdropping potentially in the wireless network. And so we call such network as directional-antennas wireless networks.

DADCQ protocol which uses the distance method for forwarding decision threshold value. The distance method is used to measure the distance to the nearest neighbor node. If the distance is greater than the threshold value then the node rebroadcast the message in network. These methods share a common framework where the nodes measure the value of the variable at their location and they calculate a threshold value using the variables and make a rebroadcast determination based model on whether or not value of the variable exceeds the value of the calculated threshold. The behavior of the distance method protocols is largely determined by the particular protocol parameter called as Dc [8].The distribution pattern of the network is independent parameter

of the density but can also vary. As considered in case of isolated highways the nodes will be very restricted along the one dimensional path in the network. Where as in the urban area network the nodes may appear in the pattern which is the more uniformly distributed in two dimensions. And so the road crossings and suburban areas can exhibit many combinations in between in VANET network. And so the broadcast protocols of network should be able to function equally well in all these scenarios of the VANET network.

Furthermore the vehicles can use wireless communications for the vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communications in network [9].Another problem in wireless communication and VANET in particular is the loss of packets in the network as they travel through the medium. The multipath fading also causes the signal to interfere with itself in the work as the signal gets splits into multiple paths during traverse in the network. The reason for multipath fading is due to signal being reflected..The packets can also be lost due to interference of the different transmitted signals which each other which gives rise to a phenomenon called collision.

VANET applications includes such as traffic data dissemination which utilize broadcast as primary mode for their communication. So thus creating efficient broadcast schemes which are very important for supporting the practical VANETs [2].As this communication is between the mobile vehicles is adhoc communication in which the connected nodes can move freely in network so no wires are required for this communication. The typical examples are deployed in military or battlefield operation and also in VANET [3]. The Router Road Side (RSU) is device that connects the vehicles present on the road and it also connects to other network devices present in the network. So each of the vehicle consists of On board unit(OBU) which connects to the vehicle with RSU through DSRC radios and the other device is which is Tamper Proof Device (TPD) which holds the vehicles secrets information such as information about vehicle like key, driver identity, trip detail, speed, route details etc.And as approximately the number of vehicles are exceeding 750 million in the world till today. Also the vehicular mobility model plays a significant role in evaluation of the different challenges present in the scenario in the network [4].Today these VANET vehicles will require a authority to govern the system present in it. In the VANET each vehicle is able to communicate with the other vehicle using the short radio signal detected using a short range communication (DSRC) which is operating on 5.9 GHz in range of 1 KM.As the High vehicle mobility and the frequent topology changes in VANET have very negative influences on performance of the data distribution in such kind of the network.[5].

II. Measuring the Spatial Distribution

DADCQ protocol supports the broadcast application in for 1D and 2 D distributions so we need to find the way to adapt the threshold function in such as way to adapt in dynamic manner for 1D and 2D distributions. For this we need method to dynamically measure the distribution pattern. So the science of analyzing the nodes distribution is called as spatial distribution. A quadrant function is used to characterize the node distribution pattern. The quadrant method is used to measure how evenly the nodes are spaced in the network. A point or the node can be regularly spaced such as in lattice or clumped position or somewhere else in between them. This method addresses problem by inspection of frequency pattern of the nodes. There are two basic types of quadrant censusing and quadrant sampling censusing.Censusing divides the space into equally sized cells and count the number of points in each of the cell in the network. The result of the census in which array nm, indicates the count m how many cells have m nodes in them. For example if n_8=9 nine cells contains eight nodes. In the sampling process the cell position is random and also the location is random and nodes within it are counted some number of times. The sampling produces the result frequency array n_m. As per the study shows that in wireless broadcast protocol the when the area is being measured and the number of sample points are small so the sampling seeks be a better than the censusing. Selecting the values for the number of samples and the cell size is complicated one and it does not have a one size fits all solution. Here the sample size is chosen as 30 and a circular cell and radius r=5 where r is the radius of transmission. So the process of calculating the frequency values for n_m is as follows:

1. Initialize n_m =0 for m= [0, N].
2. Generate random point, y within the node's transmission area, set=0.
3. For each neighbor and the node itself, if it is within r/5 of x, y increment m.
4. Increment n_m.
5. Repeat steps 2-4 for 30 times.

Once frequency array is computed then we need to create a single value to represent the result. And if the distribution is 2D is uniformly random then the values in n_m will follow a Poisson distribution is that the mean is equal to the variance.

III. Removal and Reduction of Eavesdropping by Global Predictor(GI)Method

As discussed earlier eavesdropping are very critical attacks in the wireless network and it difficult to detect the eavesdropping nodes. So for the detection of eavesdropping attack removal we have used Global Predictor (GI) method so as to detect the eavesdropper nodes in the VANET.The procedure of the Global Predictor (GI) method is as follows:

1. Select a number of number for random VANET
2. Make one node as a Global Predictor (GI) node
3. Select the Transmitter node
4. Select the Receiver node
5. First transmitter node will transmit the data in encrypted form to the Global Predictor (GI) node
6. Global Predictor (GI) node will store the data transmitted by transmitter node in encrypted form and it will encode the data.
7. Now all the communications will be made through Global Predictor (GI) node and no single node is allowed to communicate individually with each other.
8. If the communication occurs other than Global Predictor (GI) node than it will not considered as a valid communication i.e. an eavesdropper node is found and it will be removed from the network.

IV. Result

As shown in the Fig. I the random nodes are generated in the NS-2 simulator in which Global Predictor (GI) node is set with the blue color as indicated in the random nodes generation and the other nodes such transmitter node is of red color and receiver color is green color.

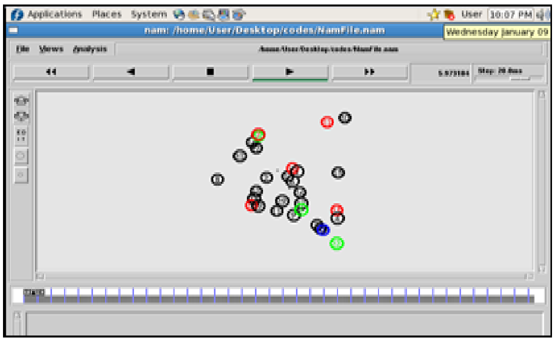

Fig I. Random nodes without Global Predictor (GI)

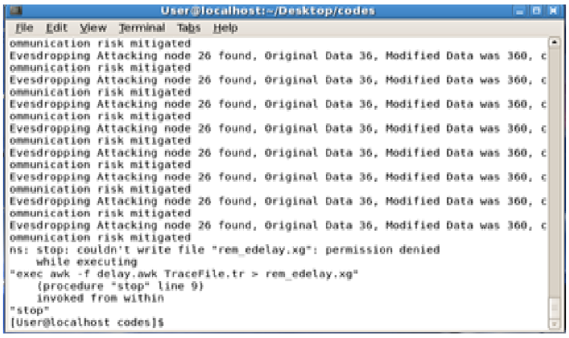

Fig II. Eaves Dropping without Global Predictor (GI)

As seen in the Fig I we have not applied any method to prevent the eavesdropping attack in the network and so the result of which gives rise to the packets drop between the sender and the destination nodes and moreover the Global Predictor(GI) is not been applied for the communication in the network so there is unauthorized access to the transmitting data from the source to destination path and these nodes being attacked by the eavesdropper nodes and which being detected and identified in the simulation as shown in the Fig II which shows the data regarding the eavesdropper node and its number. So the first and the foremost job is to block these malicious nodes and the use the Global Predictor method(GI) for the transmission of data between the sender and the destination nodes.

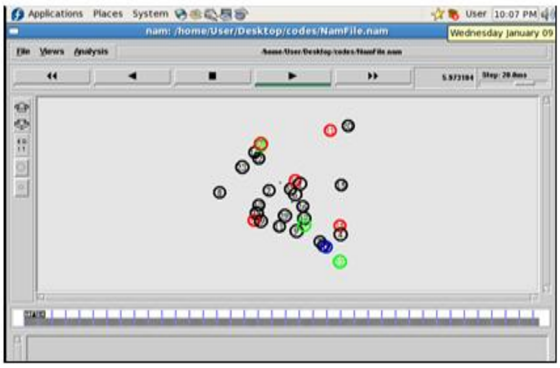

Fig III. Eaves Dropping with Global Predictor (GI)

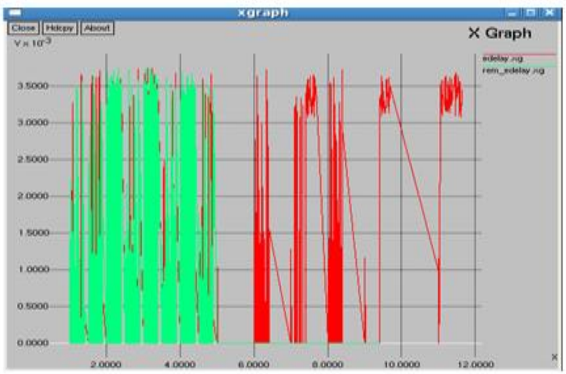

Fig IV. Energy Eaves Dropping Delay

After 6 weeks of follow upmit was found that LDL-C ,

As shown in the Fig. III. we have applied the Global Predictor (GI) method and because of which the whatever data transmission is going to happen is going to be happen through the universal node that means the universal node that is as shown in simulation which is of color blue will act as the intermediate node between the source node and the destination node. So all the communications which are happening through Global Predictor (GI) will only be considered and rest all will not be considered that those are the eavesdropping coummications.

As seen from the Fig IV. When the eavesdropping happened then the delay in the communicating between the sender and the destination node is more which shown in the Fig IV. On the contrary when the there is no eaves dropping in the network that not a single node is been affected with the eavesdropper node than the delay will be less as shown by the green portion in the Fig IV.Whereas the red portion indicates the delay which is caused by the eavesdropper nodes and so the delay is more. So after the application of Global Predictor (GI) method the delay has been reduced a great extent as shown in the Fig IV.

V.Conclusion

Thus we have detected the eavesdropper nodes and masked the eavesdropper node while transmission or reception of the date from sender node to destination node by using the Global Predictor(GI) method which acting as a universal node in the wireless network all the communications are happening through this node. And we have also reduced the delay during the transmission of the signal after applying the above network as shown in the simulation results.

References

[1]. 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.

[2]. "Hadoop Distributed File System."[Online].Available:https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html. [Accessed: 14-Sep-2017]

[3]. "MapReduce." [Online]. Available: https://hadoop.apache.org/docs/r1.2.1/mapred_tutorial.html. [Accessed:23-Sep-2017].

[4]. S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, "A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks," IEEE CommunicationsLetters, vol. 20, no. 4. pp. 700–703, 2016.

[5]. J. U. Santhi, S. Bellamkonda, and N. G. Rao, "Analysis of web serverlog files using Hadoop MapReduce to preprocess the log files and toexplore the session identification and network anomalies," in 3rdInternational Conference on Electrical, Electronics, Engineering Trends,Communication, Optimiza tion and Sciences (EEECOS), 2016, pp. 856–861.

[6]. J. Pescatore, "How DDoS Detection and Mitigation Can Fight AdvancedTargeted Attacks," Sans Institute, 16p., 2013.

[7]. G. Zhang, S. Jiang, G. Wei, and Q. Guan, "A prediction-based detectionalgorithm against distributed denial-of-service attacks," in Proceedingsof the 2009 International Conference on Wireless Communications andMobile Computing Connecting the World Wirelessly - IWCMC '09,2009, pp. 106–110.

[8]. A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detectionagainst network mimicking DDoS attacks," IEEE CommunicationsLetters, vol. 13, no. 9. pp. 717–719, 2009.

[9]. Y. Chen, X. Ma, and X. Wu, "DDoS Detection Algorithm Based onPreprocessing Network Traffic Predicted Method and Chaos Theory," IEEE Communications Letters, vol. 17, no. 5. pp. 1052–1054, 2013.

[10]. M. T. Rosenstein, J. J. Collins, and C. J. De Luca, "A practical methodfor calculating largest Lyapunov exponents from small data sets," Physica D: Nonlinear Phenomena, vol. 65, no. 1, pp. 117–134, 1993.

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

[12]. 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.

[13]. Angiulli, F., Fassetti, F., "Detecting distance-based outliers in streams of data", In: Proceedings of the Sixteenth ACM Conference on Information and Knowl- edge Management, ACM, pp. 811-820, 2003.

[14]. Sunny Behal, Krishan Kumar , Monika Sachdeva, "Discriminating Flash Events from DDoS Attacks: A Comprehensive Review", InternationalJournal of Network Security, Vol.19, No.5, PP.734-741, 2017

[15]. K.Giotis, C.Argyropoulos, G.Androulidakis, D.Kalogeras, V.Maglaris,"Combining OpenFlow and sFlow for an effective and scalable anomalydetection and mitigation mechanism on SDN environments", Computer Networks Volume 62, pp.122-136, April 2014

[16]. Paul Goransson, Chuck Black, Timothy Culver, "How SDN Works",Software Defined Networks, pp.61-88, 2017

[17]. Ahmed Abdelaziz, Tan Fong Ang, Mehdi Sookhak, Adnan Akhunzada, "Survey on Network Virtualization Using OpenFlow: Taxonomy, Opportunities,and Open Issues", KSII Trans. Internet Inf. Syst., vol. 10, no.10, pp. 4902-4932, 2016.

[18]. Y. Feng, R. Guo, D.Wang, and B. Zhang, "Research on the Active DDoS Filtering Algorithm Based on IP Flow", in 2009 Fifth InternationalConference on Natural Computation. IEEE, 2009, pp. 628-632, 2009.

[19]. Neumann, Peter G, "Denial-of-Service Attacks", Communications of the ACM, p. 136. Academic OneFile, Aug 2017.

[20]. https://en.wikipedia.org/wiki/Normal distribution.

Dharmaveer P. Choudhari. " Eavesdropping Detection and Removal for Spatial Distribution and Channel Quality Adaptive Protocol in VANET" IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 44-47.