International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 2, March - April 2016 **ISSN 2278-6856**

DETECTION AND PREVENTION OF MALICIOUS NODE USING DATA CENTRIC TECHNIQUES

[1] Adity , [2] Dalveer Kaur

[1].Department of C.S.E LPU, Phagwara Punjab

[2.] Assistant Professor Department of C.S.E LPU, Phagwara Punjab

ABSTRACT

VANET is used in order to transfer the data from mobile source to mobile destination. This type of communication is desired in now days world. The reason for this is lack of time. As more and more users come into contact with the VANET, the security is at stakes. The proposed paper deals with this security issues by the use of DMN (Detection of Malicious Node) using data centric techniques. The proposed technique tries to uncover the maliciousness by the use of packets which are transferred from source to the destination. The results show the proposed technique handle the security issues better as compared to the existing system.

Keywords:-VANET, Security, Malicious, Packets, DMN, Data Centric

1. Introduction

VANET is Vehicular Ad-hoc Network. The principal of MANET is used in case of VANET. MANET means mobile ad-hoc network. VANET is commonly used as inter vehicle communication. [1] Communication in Vehicular ad hoc Network relies on exchange of information among different vehicular nodes in the network. This helps to improve the safety, driving efficiency and comfort on the journey for the travelers. In this network, information received from other vehicles is utilized to make majority of the decisions. However, a node may behave malicious or selfish in order to get advantage over other vehicles. A misbehaving node may transmit false alerts, tamper messages, create congestion in the network, drop, delay and duplicate packets. Thus, detecting malicious nodes and data in VANET is very crucial and indispensible as it might have disastrous consequences. The suggested paper[1] provide a detailed survey on some of the important research works proposed on detecting misbehavior and malicious nodes in VANETs. In addition to the details about the techniques used for misbehavior detection, nature of misbehavior, this paper categorizes the schemes for better understanding and also outlines several research scopes to make VANET more reliable and secure. [2] Numerous local incidents occur on road networks daily, many of which may lead to congestion and safety hazards. If vehicles can be provided with information about such incidents or traffic conditions in advance, the quality of driving can be improved significantly in terms of time, distance, and safety. [2]Vehicular Ad Hoc Networks (VANETs) have newly emerged as an effective tool for improving road safety through the dissemination of warning messages among the vehicles in the network about potential obstacles on the road ahead.[2] Various Approaches of data dissemination in vehicular network can be used to inform vehicles about dynamic road traffic condition so that a safe and efficient transportation system can be achieved. Here we extensively reviewed various data dissemination techniques and identify the challenges with it. However, type of VANET applications and inherent VANET characteristics such as different network density, fast movement of vehicles make data dissemination quite challenging. VANET is shown in the fig 1.

When data is transferred over the VANET than there are number of problems which can occur. All of these problems are tackled in the proposed algorithm. The propose algorithm uses data centric techniques in order to overcome the problems present within the VANET. The data centric techniques will increase the overall performance of the transmission over the VANET. It will be easy to detect the malicious data when these techniques are implemented. The concept of CA(Certification Authorities) will be used in order to inspect the various nodes which are involved in the data transmission. Generally data centric techniques are implied on the sender nodes only.

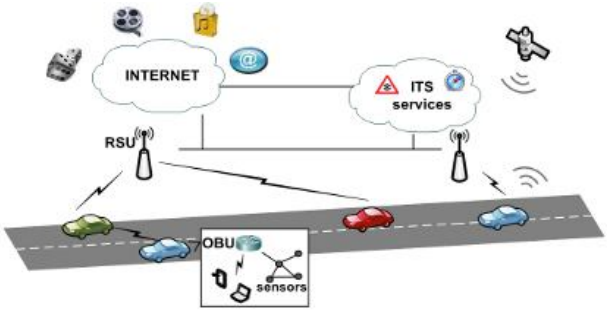

Fig 1: Showing utilization of VANET and use with Internet

Data centric techniques can be used in order to tune the data. Once the data is tuned then it will be delivered to the destination. The quality of the data will be increased by the use of data centric techniques. The combination of data centric techniques along with the VANET is used in order to enhance the performance of the system. VANET is exposed to various attacks. [3] VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. [3]This paper presents a survey of VANETs attacks and solutions in carefully

considering other similar works as well as updating new attacks and categorizing them into different classes. The attacks are categorized into number of categories.

1.1) Malicious Attacker

This type of attack is used by the attacker to damage the member node. There does not exists any personal benefit of the attacker.

1.2) Rational Attacker

This type of attack is similar to malicious attacker with the difference that personal benefit of the attacker is involved in this case.

1.3) Active Attacker

Active attacker is the one who generate the new packets in order to harm the network.

1.4) Passive Attacker

This type of attacker can only perform eavesdropping.

1.5) Local Attacker

Local Attacker will be the one who has limited scope. In other words the local attacker has limited region of attack.

1.6) Extended Attacker

This type of attacker will be the one who has larger scope as compared to local attacker. More regions are covered in this case.

1.7) DDOS

This attack is also very common. In this attack the files are replicated over the network which will cause traffic on the network to enhance. This will cause the network to cease down and resources are not available to the user as required.

The proposed work covers the various types of attacks and their solutions as well.

2. Review of Literature

In order to suggest the proposed work lots of papers have been analyzed. Some of the papers which we have studied and are relevant [2] include the mechanism to determine the traffic on the road. This paper also indicates that how congestion over the network and what mechanisms can be followed to improve the flow of the traffic. The mechanism suggested in this paper is expensive in nature. Also there is no means to impose any fine in case of malicious node. Also malicious node is not blocked. [3] Data centric techniques are considered in this case. In this paper the focus is set on the data which is transferred over the VANET. Data centric technique prevents the transferred of the same data again and again over the VANET. The suggested technique in this case is expensive in nature. Also malicious node is not blocked. [4] It is difficult to manually identify opportunities for enhanc- ing data locality. To address this problem, we extended the HPCToolkit performance tools to support data-centric pro- filing of scalable parallel programs. Memory access latency is measured by the use of hardware counter. Technique suggested is expensive in nature and the malicious nodes are not blocked. [5] security is considered in this case. When data is transferred over the VANET then it is possible that attack will occur. Various attacks are considered in this case. The most common attack over the VANET is DDOS. With this attack the resources are blocked and they are not available to the users when they require them. The method will be suggested in order to stop DDOS but nothing is done in order to permanently block the nodes causing the problems. [6] Security is one in all the main problems in VANET. Cooperation among inter-vehicular networks and device networks placed inside the vehicles or on the road need to be further investigated and analyzed. As the number of vehicles grows the trust between them should also be maintained for the flexible communication. There are lots of analysis regarding VANET for driving services, traffic data services, user communication and knowledge services. This network, with its huge size, plays a critical role in communication because all types of people use it to achieve daily routine required service. The mechanism which is considered is expensive in nature. [1] VANETs enable wireless communication among vehicles and vehicle to infrastructure. Its main objective is to render safety, comfort and convenience on the road. VANET is different from ad-hoc networks due to its unique characteristics. However, because of lack of infrastructure and centralized administration, it becomes vulnerable to misbehaviors. This greatly threatens different aspects of VANET's security. VANET being such a useful network must provide adequate security measures for secure communication the detection of malicious nodes will be considered in this case. The technique which is used is known as node centric technique. Suggested technique is expensive in nature. [7] Various challenges associated with the VANET are considered in this case. When data is transferred over the network then chances of leakage of data is always present. Various threats and there solutions are considered in this case. The most common attack which takes place over the network is not considered. That attack is DDOS. Prevention mechanisms are not specified in this case. [8] Vehicular Ad Hoc Networks (VANET) has mostly gained the attention of today's research efforts, while current solutions to achieve secure VANET, to protect the network from adversary and attacks still not enough, trying to reach a satisfactory level, for the driver and manufacturer to achieve safety of life and infotainment. The need for a robust VANET networks is strongly dependent on their security and privacy features, which will be discussed in this paper. In this paper a various types of security problems and challenges of VANET been analyzed and discussed; we also discuss a set of solutions presented to solve these challenges and problems. [9] This paper presents a class of routing protocols called road-based using vehicular traffic (RBVT) routing, which outperforms existing routing protocols in city-based vehicular ad hoc networks (VANETs). RBVT protocols leverage real-time vehicular traffic information to create road-based paths consisting of successions of road intersections that have, with high probability, network connectivity among them. Geographical forwarding is used to transfer packets between intersections on the path, reducing the path's sensitivity to individual node movements. For dense networks with high contention, we optimize the forwarding using a distributed receiver-based election of next hops based on a multi criterion prioritization function that takes non uniform radio propagation into account. We designed and implemented a

reactive protocol RBVT-R and a proactive protocol RBVT-P and compared them with protocols representative of mobile ad hoc networks and VANETs. Simulation results in urban settings show that RBVT-R performs best in terms of average delivery rate, with up to a 40% increase compared with some existing protocols. In terms of average delay, RBVT-P performs best, with as much as an 85% decrease compared with the other protocols.

3. PROPOSED SYSTEM

There could be different types of nodes which exist over the VANET. All the nodes which exist over the VANET can have different types of attributes and behavior associated with them. The main objective of the proposed system is to permanently block the node which is detected as malicious. In our work first of all we will detect the DDOS attack and then rectify the problem using filtering and selective data transmission. An authentication mechanism is used in order to verify the honest node. A malicious node will duplicate the packet and hence increase the traffic in the network. We will also check the packets for validation. Data centric technique will be used in this case. The packet which is received by the receiver and transmitted by the sender will be compared in order to verify their validity. The protocol which is followed in this case will be DMNDC(Detection of Malicious Node using data centric technique). The prime objectives which are satisfied in the proposed paper include.

a) Detection of the malicious nodes. The malicious nodes are the nodes which are going to infect the entire network and may cause the network to go down.
b) Decreasing the redundancy associated with the data packet transmission. This is accomplished with the help of validation of data.

4. RESULTS

The proposed system deals with the detection of the malicious node using the packet which is being transferred. The proposed system is implemented using the MATLAB. The figures show the result of the simulation

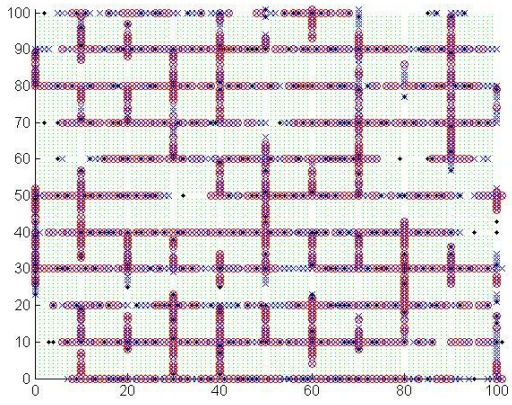

Fig 2: Showing the Packets which is transferred from source to the destination

The results with different node configuration will be as follows

Node	Average	Slandered

Configuration	Number of iterations	Deviation
True Node=6 Fake Node=3	207.05	7.86
True Node=6 Fake Node=4	227.55	6.33
True Node=6 Fake Node=5	255.8	6.26
True Node=6 Fake Node=6	304.7	7.55

Table 1: Showing the Node configurations and Average number of iterations required to detect malicious node

When the proposed method is utilized then the redundancy present within the data is reduced. Also the malicious node is going to be detected. The result is depicted with the tabular structure as follows.

Table 2: Showing Various parameters of the Existing and Proposed Work

Parameters	DMN	DMNDC
Redundancy(200 Packets)	200 Packets Transferred	160 Transferred
Malicious Nodes	10(30 Simulations)	15(30 Simulations)
Nodes Blocked	None	15
Efficiency	Low	High

The above result shows that the proposed system performs better as compared to existing system in current environment.

5. CONCLUSION

The proposed system handles the various attacks on the VANET efficiently. In the existing papers malicious node is identified. The malicious node is identified by the use of the CA. the certification authority is going to decide whether the node is malicious or not. The malicious node than will be imposed upon with the fine. But after paying the fine, node is again allowed to enter into the VANET. Also technique which is suggested is expensive in nature. The problem will start to appear when CA itself is malicious. In the proposed system all of these problems are tackled. The sending machines are monitored by the inspecting devices. In case of any misbehave it is reported to the Certification Authority. It is up to the certification authority to block the node. The node if blocked will be permanent in nature. In this method a buffer is maintained. The packets which are already delivered will be stored within the buffer. The incoming packet will be compared against the packet stored within the buffer. If packets matches than they will be declared as malicious.

The tool which is used is MATLAB. The performance charts are prepared which can be used to compare the performance of the new system. There could be number of tools which can be used in order to simulate the current environment but we have chosen MATLAB as a tool to simulate the proposed system. MATLAB is based on the direct approach rather than iterative approach. Hence

solution will be obtained well within the time. The throughput generated is also very high.

REFERENCES

[1]. U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 965–972, 2015.

[2]. D. Sutariya, "Data Dissemination Techniques in Vehicular Ad Hoc Network," Int. J. Comput. Appl., vol. 8, no. 10, pp. 35–39, 2010.

[3]. N. Rutar and J. K. Hollingsworth, "Software Analysis Techniques to Approximate Data Centric Direct Measurements.," First Int. Work. High-performance Infrastruct. Scalable Tools, 2011.

[4]. X. Liu and J. Mellor-Crummey, "A data-centric profiler for parallel programs," Proc. Int. Conf. High Perform. Comput. Networking, Storage Anal. - SC '13, pp. 1–12, 2013.

[5]. V. H. La and A. Cavalli, "S Ecurity Attacks and Solutions in V Ehicular a D Hoc N Etworks□: a S Urvey," vol. 4, no. 2, pp. 1–20, 2014.

[6]. A. Pathre, C. Agrawal, and A. Jain, "Identification of Malicious Vehicle in Vanet Environment From Ddos Attack," J. Glob. Res. Comput. Sci., vol. 4, no. 6, pp. 1–5, 2013.

[7]. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommun. Syst., vol. 50, no. 4, pp. 217–241, 2012.

[8]. G. Samara, W. a. H. Al-Salihy, and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," Netw. Appl. Protoc. Serv. (NETAPPS), 2010 Second Int. Conf., pp. 55–60, 2010.

[9]. J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information," IEEE Trans. Veh. Technol., vol. 58, no. 7, pp. 3609–3626, 2009.