International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10824-10827

Technique to Detect and Isolate Jamming Attack in VANET

Gagandeep Kaur
M.Tech Student, Department of Computer Science and Engineering,
Chandigarh Engineering College, Landran, Punjab, India.
Orcid Id: 0000-0001-5820-2498

Parveen Sharma
Assistant Professor, Department of Computer Science and Engineering,
Chandigarh Engineering College, Landran, Punjab, India.

Abstract

The vehicular ad hoc network is the decentralized type of network in which mobile nodes can communicate with each other. Due to self configuring nature of the network malicious nodes join the network which are responsible to trigger various types of active and passive attacks in the network. The jamming attack is the active type of attack in which malicious node select the nodes which will be controlled by the malicious node. The selected nodes are responsible to flood the victim node with the rough data packets. In this work, threshold based technique has been proposed in which node which is sending data above the threshold value will be responsible to trigger jamming attack in the network. The proposed technique has been implemented in NS2 and it has been analyzed that proposed technique performs well in terms of throughput, delay and packet loss.

Keywords: Vehicular Ad hoc Network, Routing, Jamming Attack, Packet Delivery Ratio, Throughput.

INTRODUCTION

For the purpose of introducing the communication technology within the vehicle-specific applications lately, various projects have been evolving within the Ad-Hoc Networks [1]. The wider aspect of this is the Intelligent Transport System (ITS). The warnings related to environmental hazards, traffic and road conditions, and transmitting local information amongst vehicles is provided using the Vehicular Ad-Hoc Networks. The VANETs have some special characteristics as compared to the MANETs. The VANETs are large-scale networks in which thousands of vehicles are deployed [2]. The mobility of the vehicles can be affected by the configuration of the road, the traffic laws as well as the speed limits. As compared to the typical mobile devices which are involved in MANETs, more resources are to be accessed by vehicles in the case of VANETs [3]. The information related to link is used within the network for transferring the packets from source to destination in the case of topology based routing protocols. There are three broader classifications of these protocols which are Proactive routing, Reactive routing and Hybrid routing.

JAMMING ATTACK

The transmission of radio signals for disrupting the communications within the network deliberately is known as a jamming attack. This results in reducing the signal-to-noise ratio of the complete network [4]. For the purpose of differentiating it from the unintentional jamming, the utilization of word jamming is done. The security of the network is affected on large scale through the occurrence of jamming attack. The communication between the nodes is interrupted through the constant signals sent by the jammers. The signals being received continuously show as if the channel is busy at all durations. Therefore, no signals can be sent or received from that jammed region. The packets are sent successfully by sender after the jamming begins. However, all the packets sent by the sender are not received at the receiver end. Due to this reason the packet delivery ratio (PDR) is reduced. There are various kinds of important information related to conditions, weather, accidents and so on which is carried by the packets [5]. There are large casualties that can be caused if these packets are not sent or received as per the need. It is important to make sure that the important information is received or sent for the network to be working in a successful manner. The VANETs have higher mobility and thus the topology keeps changing in a rapid manner [6]. It is very difficult to prevent jammers to enter this network due to the fact that they do not need to comply with the other protocols and also have unlimited mobility. The jammer can either be standing on feet or can also be driving in a random manner on the roads. There is a control by the adversaries on the activation and deactivation of the jamming. These issues have made it difficult to solve or detect the jamming attack issue.

LITERATURE REVIEW

Hani Alturkostani, et.al, (2014) proposed in this paper [7] the effects caused due to the jamming on the threshold-based

agreement in VANETs. The selected decision within the network is turned out to be wrong when the jamming attack occurs within the network. There is an Emergency Electronic Brake Lights (EEBL) safety application that is utilized here for testing the jammer attack. The position and power are the factors that affect the correctness of the decision made and this can be demonstrated through the experiments. The number of vehicles present in the area is also an important factor to be considered for the occurrence of jamming attack. A novel adaptive threshold algorithm is introduced here that enhances the resilience against jamming attack. This is better than the earlier researches.

Ikechukwu K. Azogu, et.al, (2013) proposed in this paper [8], effects caused due to the presence of jamming attack within the standard V2V communications, 802.11p. Within the wireless communications, the jamming attack is a part of the DoS attack. There are various solutions proposed for these types of attacks in case of general 802.11 wireless LAN. However, fewer studies have been proposed for the 802.11p networks. Comparisons are made between the newly proposed technique and the traditional approaches and it is seen that the approach newly proposed here is suitable as per the security measures and the metrics that are to be needed for designing the security measures.

Jalel Ben-Othman, et.al, (2014) proposed in this paper [9], a new analytical model that represents the behavior of jamming attacks occurring in VANETs. The communication amongst the nodes within the network is disrupted by one single node. This node is presented by the DoS attack. This results in reduction of quality of service of the whole network. There were earlier the Markov chains utilized for representing this attack within the analytical mode. However, various issues were emerging within the network and so a need to propose a new technique emerged. The results caused due to this attack were determined by the new proposed technique. This information further helped in determining whether the DoS attack is present within the network or not.

Mohamed S. Mohamed, et.al, (2017) proposed in this paper [10], the reliability of the various safety applications when he jamming attack is present in the network. Mainly hybrid jamming is focused here which unavoidable within such technologies. A proposed study is proposed on the effects caused due to the presence of hybrid jamming on voting-based approaches. Further, an Enhanced Voting-based Algorithm is proposed which helps in solving the issues that arouse in other already existing approaches. The performance of this algorithm is measured with the help f various experiments. It is seen through the various results that in terms of the time required for making decisions and reliability this algorithm is more efficient as compared to other algorithms.

Óscar Puñal, et.al, (2013) proposed in this work [11], the proper analysis of the performance of 802.11p-based vehicular communications when the RF jamming attacks are present within them. The transmission success rate of the car-to-car link is provided within a constant, periodic and reactive RF jamming attack. Vehicular platoon is emulated for providing the outdoor measurements. The major issues arising in VANETs due to this attack are noted. It is seen through the results achieved that the communication of the network can be interrupted by the constant, periodic as well as reactive jammer within the huge network areas. This might result in affective the road safety to higher extent.

Xia Shen, et.al, (2013) surveyed in this paper [12], a collection of representative congestion control approaches for the IEEE 802.11p vehicular network. Assist, a novel distributed multi-priority congestion control method is proposed to maximize the transmission open doors for the highest priority traffics while keeping the collision probability at a low level. Open issues for the future work on the congestion control approach design are drawn in this paper. This simple proposed approach additionally gets critical gain in the system throughput performance and can be effectively to be implemented in a practical IEEE 802.11p MAC layer.

RESEARCH METHODOLOGY

This work is based on to detect the malicious nodes from the network which are responsible to trigger DDOS attack in the network. The jamming attack is the distributed denial of service attack in which malicious node chooses the legitimate node which will trigger attack on the victim node. In the DDOS attack, the malicious node will send the control packets to the legitimate nodes and legitimate nodes will send the rough data packets to the victim node to trigger attack.

In this work, threshold based technique is proposed which will detect malicious nodes from the network and to detect malicious nodes following are the steps which are followed:

- In the first step, the network is deployed with the finite number of vehicle nodes. The fixed bandwidth is allocated to each vehicle node in the network.
- The road side units start analyzing the bandwidth consumption of each vehicle node and node which is using the bandwidth above allocated value will be the malicious node.
- In the third step, the road side units check the type of packets sent by the node using the bandwidth above the allocated value. When the node is sending the data packets to the victim node, it may be the malicious node.
- In the last step, the node which is sending the rough data packets, receives control packets from any node then that node will be detected as the malicious node which is responsible to trigger jamming attack.

Threshold based Algorithm

Input: Number of vehicle nodes

Output: Detection of malicious nodes

1. Assign bandwidth the data rate to each node in the network
2. The source node start sending data to destination node
3. If (bandwidth consumption >threshold)
4. Check channel on which data rate is high than threshold
5. Check the node which is sending data packets on the node
6. If (node ==detected)
7. Check the node which is sending control packets
8. Isolate detected node
9. Else
10. No malicious node
11. End
12. End

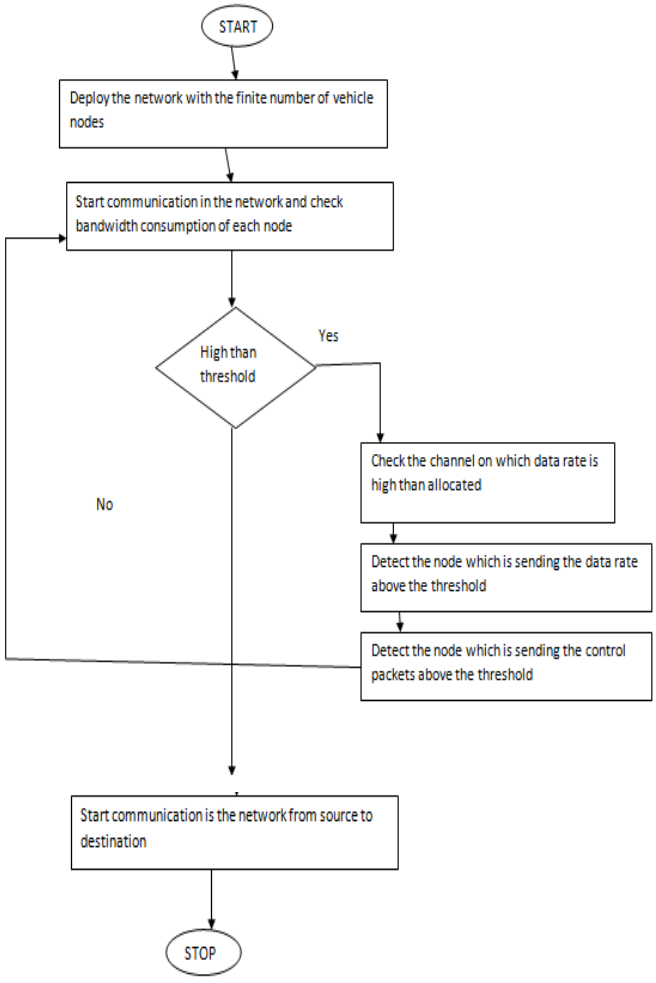

Figure 1: Flowchart of Proposed Work

EXPERIMENTAL RESULTS

The proposed algorithm has been implemented in NS-2 and the results are analyzed in terms of Routing overhead, Packet loss and throughput.

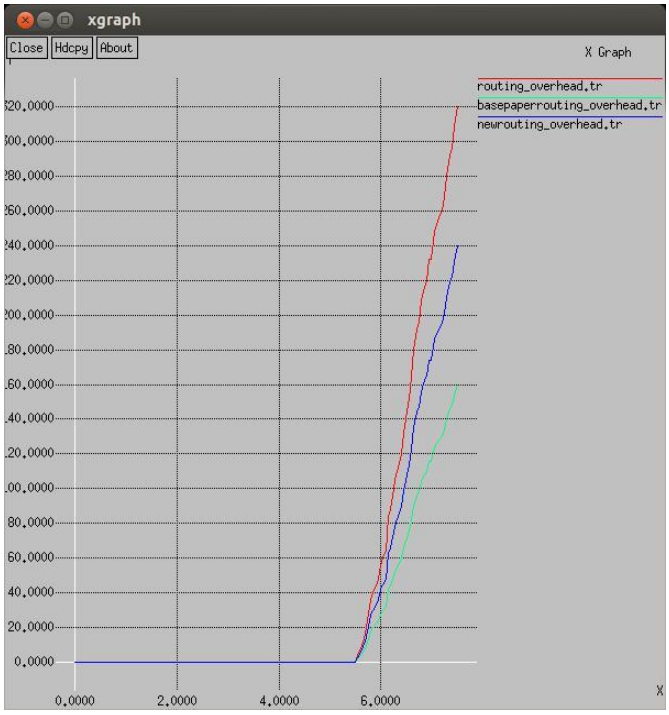

Figure 2: Routing Overhead

As shown in Figure 2, the routing overhead is compared between the existing technique, proposed technique and when the attack is triggered in the network.

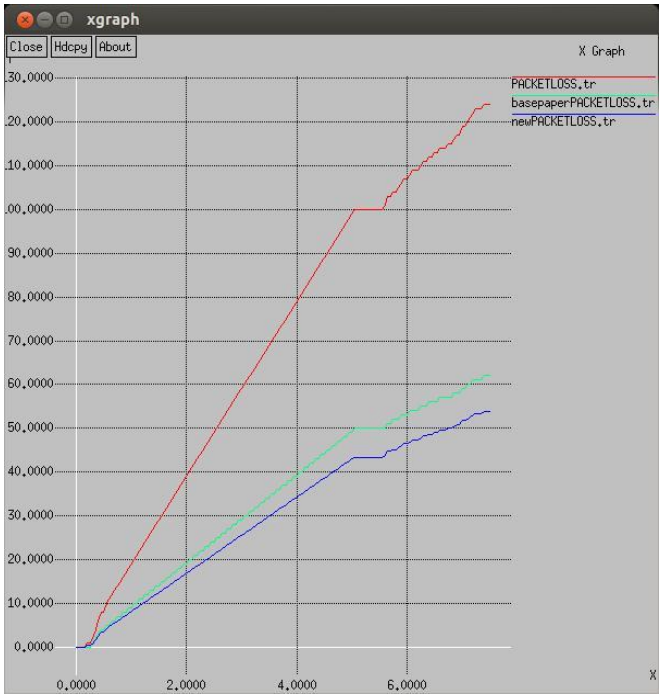

Figure 3: Packet Loss Comparison

As shown in Figure 3, the packet loss of the proposed, existing and attack scenario is compared and it has been analyzed that packet loss of the proposed technique is minimum as compared to other scenarios.

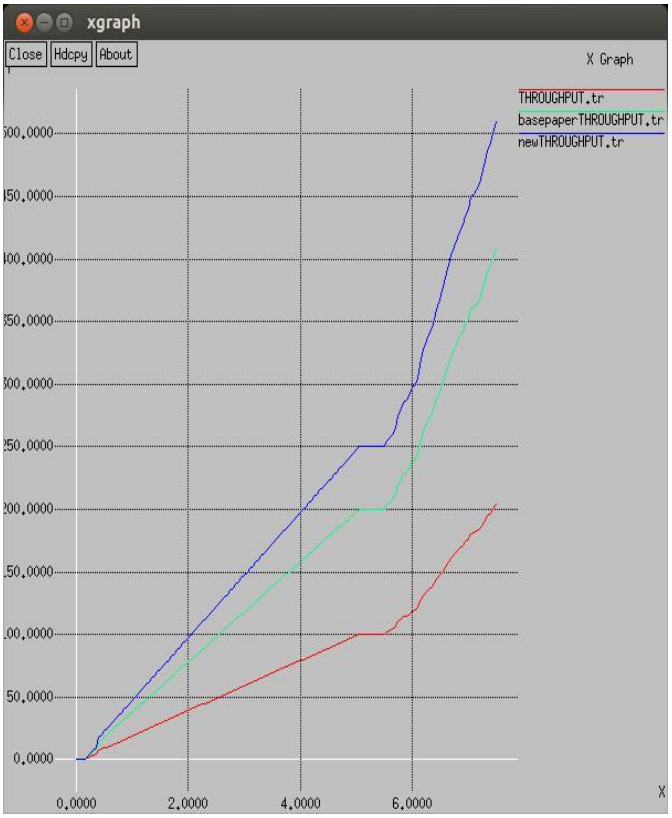

Figure 4: Throughput Comparison

As shown in Figure 4, the throughput of the proposed, existing and the attack scenario has been compared and it has been analyzed that network throughput of proposed technique is maximum due to the isolation of jamming attack.

CONCLUSIONS

In this work, it has been concluded that jamming attack is the active type of attack in which malicious node floods the victim node with the rough data packets. The malicious node joins the network because the vehicular ad hoc network is the decentralized type of network. The jamming attack is the distributed nature of attack in which malicious node chooses its victim nodes. The victim nodes start flooding the end nodes to reduce network performance. In this work, threshold based technique is proposed in which node which is sending data above the assigned value will be marked as malicious node which sends rough data packets. The proposed technique performs well in terms of various parameters. The proposed technique has been implemented in NS2 and it has been analyzed that network throughput is increased, delay is reduced, and packet loss is reduced after detection of malicious nodes from the network.

REFERENCES

[1] W Shangguang, F Cunqun, H Ching-Hsien, S Qibo, Y Fangchun," A Vertical Handoff Method via Self-selection Decision Tree for Internet of Vehicles," 2014, IEEE System Journal, doi: 10.1109/JSYST.2014.2306210.

[2] S Michael, M Imad," Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET", 2013, IEEE Trans Mobile Comput 12(4), 722–734.

[3] S Panichpapiboon, W Pattara-atikom," A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks", 2011, Communications Surveys & Tutorials IEEE 99, 1–15.

[4] Korkmaz, G., Ekici, E., Ozguner, F., and Ozguner, U.," Urban Multi-hop Broadcast Protocol for Inter-vehicle Communication Systems", 2004, ACM International Workshop on Vehicular Ad Hoc Networks, (VANET'04), Philadelphia, USA, pp. 76–85.

[5] Korkmaz, G., Ekici, E., and Ozguner, F.," An Efficient Fully Ad-hoc Multi-hop Broadcast Protocol for Inter-vehicular Communication Systems", 2006, IEEE International Conference on Communications, (ICC'06), Istanbul, Turkey, pp. 423-428.

[6] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," 2005, IEEE WONS 2005, pp. 32–41, St. Moritz, Switzerland.

[7] Hani Alturkostani, Axel Krings, "The Impact of Jamming on Threshold-Based Agreement in VANET", 2014 International Conference on Connected Vehicles and Expo (ICCVE).

[8] Ikechukwu K. Azogu, Michael T. Ferreira, Jonathan A. Larcom, Hong Liu, "A New Anti-Jamming Strategy for VANET", 2013, IEEE.

[9] Jalel Ben-Othman, and Lynda Mokdad, "Modeling and Verification Tools for jamming attacks in VANETS", 2014, IEEE.

[10] Mohamed S. Mohamed, Sherif Hussein, Axel Krings, "An Enhanced Voting Algorithm for Hybrid Jamming Attacks in VANET", 2017, IEEE.

[11] Óscar Puñal, Carlos Pereira, Ana Aguiar, and James Gross, "Experimental Characterization and Modeling of RF Jamming Attacks on VANETs", 2013, IEEE.

[12] Xia Shen, et.al," Distributed Congestion Control Approaches for the IEEE 802.11p Vehicular Networks", 2013 IEEE Intelligent transportation systems magazine.