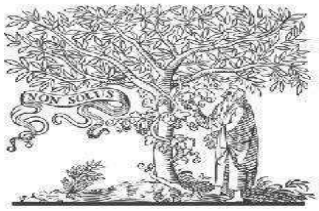
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPYRIGHT



ELSEVIER
SSRN

IJIEMR Transactions, online available on 15th Nov 2021. Link

:http://www.ijiemr.org/ downloads.php?vol=Volume-I0&issue=ISSUE-11

DOI: 10.48047/IJIEMR/VI0/111/08

Title: **Influence of Bottleneck Nodes on Malicious Packet Dropping Nodes Mitigation in Wireless Infrastructure-less Networks**

Volume 10, Issue 11, Pages: 50-53

Paper Authors

Afsha Nishat, Dr. Guddi Singh, Dr. Mohammed Abdul Bari

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Influence of Bottleneck Nodes on Malicious Packet Dropping Nodes Mitigation in Wireless Infrastructure-less Networks

[1]Afsha Nishat, [2]Dr. Guddi Singh, [3]Dr. Mohammed Abdul Bari
[1]Research Scholar, Kalinga University.
[2]Assistant Professor, CSE Department; Kalinga University.
[3]Assocate Professor, HOD Computer Science Department ISL College of Engineering, Hyderabad, Telangana, India.
[1]afsha7390@gmail.com ,[2]singh@kalingauniversity.ac.in , [3]bari_bari11@rediffmail.com,

Abstract:

Mobile ad hoc networks as an infrastructure free, and constrained resource environment network. The network aim is to establish internet connectivity everywhere regardless of location. The applications of network are healthcare, disaster relief and military, where reliable communication is major concern. Communication in the network is initiated by establishing the communication route between source and destination and sending the information through it. One of the characteristics of MANETs is a peer-to-peer network, where intermediate nodes have to cooperate for reliable communication by acting as routers. In literature number of routing protocols have been designed based on the MANET's peer to peer characteristic. However, it may not be every time true that the intermediate nodes act as faithful routers, and they may untrustworthy either due to malicious behavior or bottleneck. Number of secure protocols have been designed to mitigate malicious behavior by neglecting the bottleneck. The paper aims to define the bottleneck, and its importance in communication. Finally, how bottleneck influence on the MANETs performance during malicious nodes mitigation.

Key Words: MANETs, routing, peer-to-peer network, bottleneck

I. Introduction

MANETs stands for "Mobile Ad Hoc Networks", and it is infrastructure less networks [1]. The aim of the network to establish the internet access everywhere with minimum overhead [2]. It consists of mobile nodes with constrained resources such as memory and energy, and they are dynamically communicating via wireless communication channel. Network allow freedom to nodes regarding their mobility, any Node can arrive and vacate the network any time, and it creates the dynamic network topology. Nodes present in the network must behave in peer-to-peer manner, such that they must behave as a router to forward the data of other communicating entities [3]. Thus, the communication performance of the network depends on the faithfulness of the intermediate node.

The application of the network comprises healthcare, military, and disaster recovery [4]. These applications are very sensitive and demands reliability in communications [5]. Communication in the network is initiated by establishing the communication route between source and destination and sending the information through it. Most of the protocols designed to establishing the communication path have been measured that the nodes present in the communication path are trustworthy [6]. However, it is not correct in MANETs due to its hostile environment [7].

The nodes present in the network may act maliciously and do not follow the communication protocols specifications and they do not forward the information and drops the packets [8] (paper considers that the communication information is in the form of packets). Moreover, some of the intermediate nodes cannot handle the heavy traffic due to their insufficient resources, and they also drop the packets, and these nodes are named as bottleneck [9 ,14].

The paper aims to define the bottleneck node and its occurrence in MANET. Further paper examines the performance of current secure routing protocols developed to prevent the packet dropping nodes from communication path. Finally, paper evaluate how bottleneck influence on the MANETs performance during malicious nodes mitigation.

II. Bottleneck node

The node presents in a MANETs must act in a peer-to-peer fashion i.e., host and router. When node act as a router, then it needs to support the source and destination to communicate each other by forwarding

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

their communication information. MANETs is an infrastructure less network and constrained in terms of resources, particularly energy and memory. Moreover, the network applications do not support to recharge and/or replace the energy device. Thus, available energy must be utilized effectively. The node consists of precise memory to behave as a router to enable the communication of the other nodes. This memory holds the packets for small amount of time to process the packet, i.e., receive, make decision, and send the packets. Thus, the available memory must be utilized effectively [15-18].

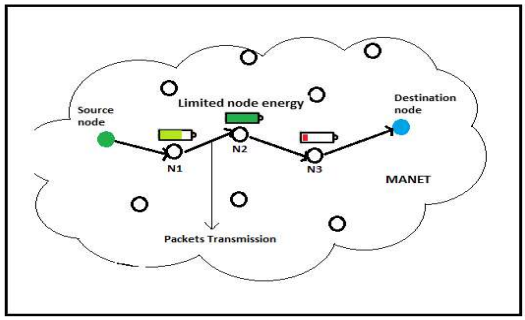


Figure 1:- bottleneck due to limited energy

During the communication if node receive the packets more than handling capacity in term of memory and energy then it drops the packets. These types of nodes paper consider as the bottleneck node. The node does not want to maliciously drop the packets but due to its insufficient resources it cannot handle the traffic and drops the packets. The bottleneck situation is happened in MANET due to the routing protocols inappropriate route-finding metric. The bottleneck nodes in MANETs shown in figures 1 and 2.

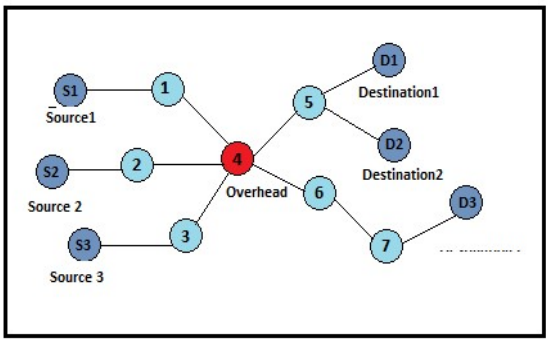


Figure 2:- Bottleneck node due to buffer overflow

III. Bottleneck influence on the MANETs performance during malicious nodes mitigation

Nodes present in the network communicate directly if both are in a communication region of one another, otherwise they need to be taken the help of intermediate nodes. Thus, the intermediate nodes need to be act as router to enable the communication. However, some of the nodes may not cooperate for communication, and they do not forward the packets and drop the packets. These nodes we considered as malicious packet dropping nodes [10].

In literature, malicious node mitigation in MANETs is majorly divided into three categories such as credit, reputation, and acknowledgement [11]. The misbehaving nodes mitigation in all three approaches is based on the packet dropping count of the intermediate node. If node drops the packet above some pre-defined threshold value, then these approaches are going to consider that particular node as malicious packet dropping nodes. They do not reflect the reason behind the packet dropping, as we discussed in previous section packets also get dropped from intermediate nodes due bottleneck [12]. Thus, we compute the performance of existing secure routing protocols performance in the presence of bottleneck nodes

Table-1: Simulation Parameters

Network-Parameters	Values
Simulation-Time	1000 s
Nodes	150
Link Layer	Logical Link
MAC	802.11
Mobility Network layer Communication.	Random SKA& PRM Two-Ray-Ground
Queue	Drop-Tail
Energy	100j
Traffic	CBR
Area of Network	1200m x 1 000m

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Performance evaluation is carried out with the help of network simulator [13]. The simulation parameters are shown in table 1. The security algorithms considered for evaluation are SKA, and PRM. Performance evaluation parameters are packet delivery fraction and packet loss. The outs of the simulations are shown in figures 3 and 4.

Simulation results shown in figures 3 and 4 clearly indicate that presence of the bottleneck intermediate node in communication path causes the sharp decrement in the performance of the network, by dropping number of packets. The existing protocols do not consider the packet dropping nodes due to constrained resources such as bottleneck intermediate node, while mitigating the malicious packet dropping nodes. If node dropping packets above the predefined value, then it treated as malicious, due to which bottle neck nodes becomes malicious and lose the chance to participate in the communication. Thus, legitimate node becomes the malicious node due to its constrained resources. Thus, the performance of the network gets decreased with respect to packet delivery.

Figure 3 shows the performance results of the IDS in terms of packet delivery fraction with respect to different data rates in the presence of reputed packet dropping nodes. In our simulation we increase the data rate by increasing the number of source and destination pairs, Performance is evaluated at each data rates. The result shows that the Performance of both the IDS decreases with the increment of data rates.

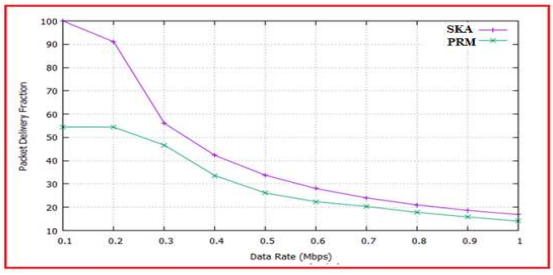


Figure 3-: PDF Performance of IDS degradation of MANET in the presence of reputed packet dropping nodes

Similarly, Figure 4 shows the packet loss of the IDS in terms of packet loss with respect to different data rates in the presence of the reputed packet dropping nodes. The result shows that the Performance of both the IDS decreases with the increment of packet loss.

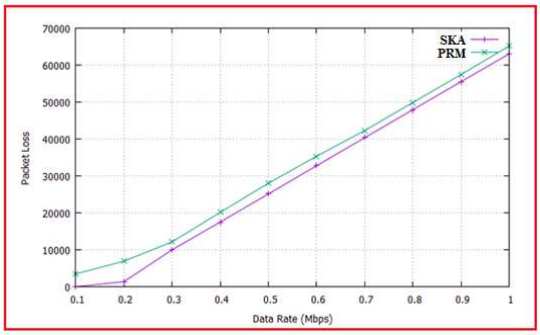


Figure 4-: Packet loss Performance of IDS degradation of MANET in the presence of reputed packet dropping nodes

Through the results, the work concludes that the reputed packet dropping node presence in the communication path is a considerable factor to enhance the IDS performance. If the existing IDS can be further implemented by the mechanism of mitigation of reputed packet dropping nodes, then the performance of the IDS improved.

III. Conclusion

Mobile ad hoc networks as an infrastructure free, and constrained resource environment network. The network aim is to establish internet connectivity everywhere regardless of location. The applications of network are healthcare, disaster relief and military, where reliable communication is major concern. Communication in the network is initiated by establishing the communication route between source and destination and sending the information through it. One of the characteristics of MANETs is a peer-to-peer network, where intermediate nodes need to cooperate for reliable communication by acting as routers. In literature number of routing protocols have been developed based on the MANET's peer to peer characteristic. However, it may not be always true that the intermediate nodes act as faithful routers, and they may untrustworthy either due to malicious behavior or bottleneck. Number of secure protocols have been designed to mitigate malicious behavior by neglecting the bottleneck. The work evaluated the performance of the secure routing protocol in presence of the bottleneck node. Finally, the work concluded that the reputed packet dropping node presence in the communication path is a considerable factor to enhance the secure routing protocols performance. If

the existing secure routing protocols can be further implemented by the mechanism of mitigation of reputed packet dropping nodes, then the performance of the IDS improved.

References:

[1] Tyagi, Sonia, and Rakesh Chawla. "Review of Routing in MANET." International Journal of Research 6, no. 7 (2019): 340-344.

[2] Dhar, Subhankar. "MANET: Applications, Issues, and Challenges for the Future." International Journal of Business Data Communications and Networking (IJBDCN) 1, no. 2 (2005): 66-92.

[3] Wadhwani, Ganesh Kumar, and Heena Khera. "Comparative Analysis of IDS and Techniques in Mobile Ad-hoc Networks." IITM Journal of Management and IT (2013): 70.

[4] Mitrokotsa, Aikaterini&Mavropodi, Rosa &Douligeris, Christos. (2006). Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks.

[5] Rafsanjani, MarjanKuchaki. "Evaluating Intrusion Detection Systems and Comparison of Intrusion Detection Techniques in Detecting Misbehaving Nodes for MANET." In Advanced Technologies. IntechOpen, 2009.

[6] Liu, Kejun, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." IEEE transactions on mobile computing 6, no. 5 (2007): 536-550.

[7] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." IEEE transactions on industrial electronics 60, no. 3 (2012): 1089-1098

[8] Siddiqua, Ayesha, KotariSridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, 2015.

[9] Sana, Afreen Begum, Farheen Iqbal, and Arshad Ahmad Khan Mohammad. "Quality of service routing for multipath manets." 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, 2015.

[10] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Mohammed Abdul Razzak. "Reactive energy aware routing selection based on knapsack algorithm (RER-SK)." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer, Cham, 2015.

[11] Mohammad, Arshad Ahmad Khan, Ali MirzaMahmood, and SrikanthVemuru. "Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network." International Journal of Hybrid Intelligence 1.2-3 (2019): 239-267.

[12] Mohammad, Arshad Ahmad Khan, Ali MirzaMahmood, and SrikanthVemuru. "Energy-Aware Reliable Routing by Considering Current Residual Condition of Nodes in MANETs." Soft Computing in Data Analytics. Springer, Singapore, 2019. 441-452.

[13] Issariyakul, Teerawat, and Ekram Hossain. "Introduction to network simulator 2 (NS2)." In Introduction to network simulator NS2, pp. 1-18. Springer, Boston, MA, 2009.

[14] Dr.Mohammed Ali Hussain and S.J. Sultanuddin Token System based Efficient Route Optimization in MANET for VANET in Smart City, Transactions on Emerging Telecommunications Technologies, January 2020 Issue, Science Citation Indexed (SCI).

[15] Dr. Mohammed Ali Hussain and Dr. Balaganesh Duraisamy Minimizing the Packets Drop by System Fault in Wireless Infrastructure less Network Due to Buffer Overflow and Constrained Energy, International Journal of Advanced Science and Technology Vol. 29, No. 5, 2020, Scopus Indexed

[16] Mohammad Arshad, Arshad Ahmad Khan Mohammad and Dr. Md. Ali Hussain Impact of Bottleneck Intermediate Node on MANETs and WSNs Performance Test Engineering and Management, Volume.83 May-June 2020, Scopus Indexed.

[17] Dr. Mohammed Ali Hussain and Dr. Balaganesh Duraisamy Preventing Malicious Packet Drops in MANETs by Counter Based Authenticated Acknowledgement Ingénierie des Systèmes d'Information Vol. 25, No. 2, April, 2020, Scopus Indexed.

[18] Mohammed Ali Hussain and D. Balaganesh Prevention of Packet Drop by System Fault in MANET Due to Buffer Overflow Intelligent Computing and Innovation on Data Science Proceedings of ICTIDS 2019, Malaysia Volume 118 Lecture Notes in Networks and Systems,