International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 6th May 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-05

Title: **IMPACT OF BOTTLENECK INTERMEDIATE NODE ON IDSPERFORMANCE IN MANETS**

Volume 09, Issue 05, Pages: 1-7

Paper Authors

MOHAMMED ABDUL BARI, ARSHAD AHMAD KHAN MOHAMMAD

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

IMPACT OF BOTTLENECK INTERMEDIATE NODE ON IDSPERFORMANCE IN MANETS

[1]MOHAMMED ABDUL BARI, [2]ARSHAD AHMAD KHAN MOHAMMAD
[1]Associate Professor; HOD CSE Department, ISL College of Engineering & Technology Hyderabad
[2]Assistant Professor, GITAM, Deemed to be University, Hyderabad, India
[1]bari_bari11@rediffmail.com, [2]ibnepathan@gmail.com

Abstract. Routing is the process to establish the communication path between communicating entities to enable communication in any networking model by forwarding the information in terms of packets. MANET is wireless infrastructure free peer to peer network. Routing in MANET is establish based on consideration that the nodes are cooperative. Malicious nodes do not cooperate for communication activities such as they drop the packets. In order to prevent malicious routing activities various intrusion detection and prevention systems designed for MANET. The main objective of these systems is to identify the malicious activities of the nodes by their packet operations. If node drops the packet more than the predefined value than it considered as malicious. But in MANET, reputed nodes also drops the packets if itbecomes bottleneck intermediate node. Thus the work aims to examine the IDS performance in the presence of bottleneck intermediate node. Further, the work shows the importance of considering bottleneck intermediate nodeduring the design of novel IDS.

Keywords: -MANETs, IDS, bottleneck intermediate node, routing, simulation.

1. Introduction

MANET [2] stands for “Mobile Ad Hoc Network”. It is a wireless infrastructure free network. Network topology of MANET is dynamic as the nodes are free to mobile. It forms multi hop communication model when source and destination do not present in a communication region of each other, and at the same time intermediate nodes need to enable the communication by acting as rooters, thus the network form peer to peer communication. Characteristics of MANETs are peer to peer communication, infrastructure free, and distributive, adaptation and self-forming. These characteristics make it to suitable for deploy at the places where, infrastructure is difficult setup and/or cost and time effective. MANET applications are disaster relief, military and emergency [5]. These fields are more sensitive and requires confidential communication [3].

In any communication environment, routing protocols are responsible for find the routing path and transfer data between the communicating entities in the form of packets. Routing protocols prime activates are establish the route and forward the information through computed route in the form of packets. Most of the routing mechanisms in MANET compute the route by assuming that the nodes are cooperative for communication [4].Malicious nodes do not cooperate for communication activities such as they drop the packets.To overcome the situation, various intrusion detection and prevention systems (IDS) are designed. The main objective of these systems is to identify the malicious activities of the nodes by their packet operations. If node drops the packet more than the predefined value than it considered as malicious. But in MANET, reputed nodes also drops the packets if it becomes bottleneck intermediate node. Nodes become bottleneck in MANET due to its constrained-resources, characteristics such as insufficient energy and buffer space, and named as reputed packet dropping nodes.

Thus the work aims to examine the IDS performance in the presence of bottleneck intermediate node. Further, the work shows the importance of considering bottleneck intermediate node during the design of novel IDS. Although there is a lot of review work has been carried out by researchers to calculate the performance analysis of IDS with different performance metrics. Our work evaluate the performance of the IDS with respect to the presence of bottleneck intermediate node. This evaluation process is the novel aspect of our work.

2. IDS for MANETs

An intrusion detection system is used to identify and prevent the unusual activities in a network, such unusual activity by intruder is violating the system security. Continuous monitoring is used to detect the unusual activities of intruders. Prevention of the intruder is achieved by various activities such as alerting the issue, and blocking the intruder. IDS is a system of procedures and activities to detect and prevent malicious activities caused by the intrudes in a communication environment. IDS also called as second line of defense for securing networking environment as it detect and prevent the system after the occurrence of intrusion.

In MANET, working of IDS is more challenging and complex in comparison with infrastructure based networks, due to MANET characteristics such as infrastructure les, absence of central coordinator, and multi-hop peer to peer networking environment. One of the considerations of routing protocols of MANET design is that nodes present in the network are cooperative for communication. It is the one of the venerable areas where nodes can compromise their security features, and attackers can gain the opportunity to provide the significant impact on the network. The major malicious activity in the MANET routing layer is the dropping the communication packets between communicating entities.

In MANETs, existing IDS designed to mitigate malicious packet dropping intruders are majorly divided into three types such as credit-based approach, reputation-based approach and Acknowledgement-based approach [6,7,8].Credit-based approach centralized approach and it is not suitable for MANET environment. Reputation and ACK based approach identifies the intruder by monitoring process of packet operations and majorly depend up on the monitoring component and process of the packet operations [9,10].

All these approaches mitigate the packet dropping nodes from the communication path [11,12]. However, all packet dropping nodes may not always drop the packets due to malicious activates but they may also drop the packets due to MANET constrained resources, and/or system failure. Due to the operation IDS, reputed nodes become malicious and it greatly negative impact on the system performance. One of the major reasons for reputed nodes drop the packets is to become bottleneck during multi hop communication, due to its constrained resources. Whenever the node become bottleneck intermediate node then it receive the packets more than its handling capability with respect to buffer and energy. Here node drops the packets due to two reasons; first one is if it receives the packets more than it’s handling capability with respect to buffer and energy, and if the packet arrival at input queue is more than its buffer capacity. Second one isit drops the packets due to insufficient energy and transmission power. Existing IDS designed based on monitoring do not recognize the packet drop due to bottleneck intermediate node.

Ayesha et al [1] designed IDS named secure knowledge algorithm to prevent the bottleneck intermediate node along with malicious packet dropping nodes. In this approach, whenever IDS monitoring component detects the packet dropping node, then it investigates the reasons behind the packet drops such as buffer overflow, lack of energy and transmission power. If investigation conform that the node did not drop the packets due to these reasons then IDS declare packet dropping node as malicious packet dropping node. However, the IDS did not prevent the node to become bottleneck intermediate node to drop the packets due to buffer overflow, lack of energy and transmission power. Thus, the paper investigate the IDS-secure knowledge algorithm performance in presence of bottleneck intermediate nodes present in the communication path.

3. PerformceIDS-secure knowledge algorithm

The aim of the paper is to investigate the IDS-secure knowledge algorithm performance in presence of bottleneck intermediate nodes present in the communication path. Performance evaluation is carried out by network simulator 2 [13]. For simulation, we consider the MANET environment with 100 mobile nodes with heterogeneous with respect to resources. Nodes are distributed in wireless communication area of 1200m x 1 000m. Randomly we select some of the nodes are malicious packet dropping nodes, which simply drop the packets and some nodes are bottleneck nodes, which drops the packets due to either constrained resource or system failure. Communication in the network starts with, source sends the constant bit rate (SBR) packets to destination. The simulation parameters are shown in Table 1.The paper evaluated the performance of the network with respect to packet delivery fraction and packet loss, and the results are shown in Figure 1 and 2.

Table-1: Simulation Parameters

Network-Parameters	Values
Simulation-Time	1200 s
Nodes	100
Link Layer	Logical-Link
MAC	802.11
Mobility Network layer Communication.	Random-way-point IDS-SKA Two-Ray-Ground
Queue	Drop-Tail
Energy	100j-150j
Traffic	CBR and TCP
Area of Network	1200m x1 000m

Through result one can conclude that importance of considering bottleneck intermediate node for design effective IDS. Not considering bottleneck intermediate node in IDS negatively impact on the network performance and effect the other networking parameters and wastage the resources of network. Moreover, reputed nodes lost the credibility to participate in communication, as IDS consider the packet dropping nodes as malicious without conforming whether it drops the packets due to malicious activities or constrained resources. That interns negatively impact on the performance of the network in terms of packet delivery and packet loss.

Packet delivery fraction of IDS-SKA is shown in figure 1 with respect to increasing data rates in the presence of malicious packet dropping, bottleneck intermediate nodes ad reputed nodes. The performance of IDS-SKA is greatly affected by the presence of bottleneck intermediate nodes.

Similarly,Packet loss performance of IDS-SKA is shown in figure 2 with respect to increasing data rates in the presence of malicious packet dropping, bottleneck intermediate nodes ad reputed nodes. The result shows that the packet loss of the IDS-SKA increases with the presence of bottleneck intermediate nodes.

Through simulation results of Figure 1 and 2, the paper concludes that the presence of bottleneck intermediate nodes during communication is not negligible factor during IDS design. Thus the IDS-SKA performance can be further improved by mitigating the bottleneck intermediate nodes along with malicious packet dropping nodes.

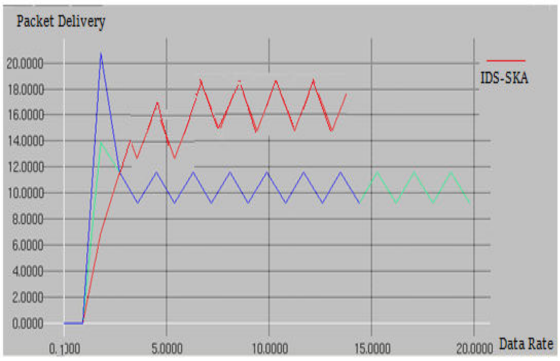

Figure 1-: Packet Delivery Performance of IDS-SKAin MANET in the presence of bottleneck intermediate nodes

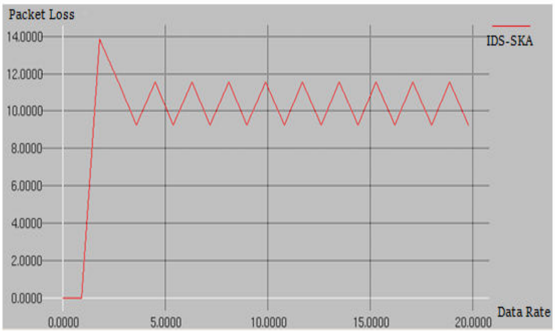

Figure 2-: Packet loss Performance of IDS-SKA in MANET in the in the presence of bottleneck intermediate nodes

4. Conclusion

Routing in MANET is establish based on consideration that the nodes are cooperative. Malicious nodes do not cooperate for communication activities such as they drop the packets. In order to prevent malicious routing activities various intrusion detection and prevention systems designed for MANET. IDS aim is to identify the malicious activities of the nodes by their packet operations. If node drops the packet more than the predefined value than it considered as malicious. But in MANET, reputed nodes also drops the packets if it becomes bottleneck intermediate node. Thus the work examinethe IDS performance in the presence of bottleneck intermediate node. Further, the work conclude the importance of considering bottleneck intermediate node during the design of novel IDS.

REFERENCES

1. 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.

2. Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." Indian Journal of Science and Technology 9 (2016): 26.

3. 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

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

5. 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.

6. Wadhwani, Ganesh Kumar, and HeenaKhera. "Comparative Analysis of IDS and Techniques in Mobile Ad-hoc Networks." IITM Journal of Management and IT (2013): 70.

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

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

9. 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.

10. 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.

11. Thachil, Fidel, and K. C. Shet. "A trust based approach for AODV protocol to mitigate black hole attack in MANET." In 2012 International Conference on Computing Sciences, pp. 281-285. IEEE, 2012.

12. Ukey, AishwaryaSagarAnand, and Meenu Chawla. "Detection of packet dropping attack using improved acknowledgement based scheme in MANET." IJCSI International Journal of

Computer Science Issues 7, no. 4 (2010): 12-17.

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.