Intrusion-Detection in Self Motivated Topology for Manets

C.M.Nalayini
Department of Information Technology, Velammal Engineering College.
Email: nalayinicm13@gmail.com
RitigaAgarwal
Department of Information Technology, Velammal Engineering College.
Email: rithika1298@gmail.com
SumaiyaHayath
Department of Information Technology, Velammal Engineering College.
Email: sumaiyahayath97@gmail.com

----------ABSTRACT----------

Mobile Ad hoc networks (MANETs) are vulnerable to having compromised operationsdue to a wide range of security attacks because of the features like unreliability of wireless links between nodes, rapidly changing topology, limited battery backup, lack of centralized control and others. New kinds of Distributed Denial-of-Service (DDoS) attacks have exhibited potential to disconnect communication networks, even cutting off entire countries from the Internet. The current study is influenced by the fact that topology changes in a network are generally expensive and slow. Nodes may misbehave either because they are malicious and deliberately wish to disrupt the network, or because they are selfish and wish to conserve their own limited resources such as power. Here we present a mechanism that enables the detection of nodes that exhibit packet forwarding misbehavior. This approach is based on the usage of two techniques which will be used in parallel in a way that the results generated by one of them are hence processed by the other in order to finally obtain the list of misbehaving nodes. The first half detects the misbehaving links with the help of the 2ACK technique and this information is fed into the second half which uses the principle of conservation of flow (PFC) technique to detect the misbehaving node. The problem with 2ACK algorithm is that it can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link are misbehaving. Using AODV routing protocols and finds one way Acknowledgement using Path Tracing algorithms to overcome the problem in our mobile wireless network.

Keywords - **MANET, AODV, DDoS, PFC, 2ACK Technique.**

I. INTRODUCTION

A Mobile ad hoc network (MANET) is a group of independent mobile nodes that are able to communicate with one another in the absence of a fixed infrastructure. Everynode in a MANET network is independent and can randomly move in any direction (dynamic), and will therefore change its links with the other nodes frequently. All the nodes are required to perform forwarding of data packets unrelated to their own use, and therefore act as a router. This type of network supports multi hop routing, an autonomous and decentralized administration, dynamic changes in the network topology, an energy limited operation and network scalability. With respect to MANET, reactive routing protocols are more suitable than proactive routing protocols as they have a reduced overhead to attacks including eavesdropping, black hole, malicious, denial of service etc. The majordrawback in constructing a MANET is to ensure that each node holds the updated information about its neighbour nodes, owing to the frequently changing nature of MANET topology. The autonomous feature of ad hoc nodes is also responsible for the motivation of attacks. These nodes are free to move anywhere in a wireless environment and can join or leave a network at any time. They are not fully secured and can be compromised, confined or hijacked by any attackers. No central authority is present and it is assumed that all participating nodes have a ccooperative nature. Many algorithms were proposed to ensure the node co-operation. The main objective of the attacker node is to destroy the cooperativeness of the ad hoc nodes. Therefore, we exploit the ARAN routing protocol to implement in our proposed work.

II. TYPES OF ATTACKS IN MANET

The attacks in MANET are broadly classified into active and passive. In a passive attack, the attacker only reads the data being exchanged in the network but does not alter it. While in an active attack, the attacker not only reads but also alters the data. There is also another classification based on the nodes involved in the attack. They are external and internal attacks. External attacks are carried out by nodes which are not a part of the network while internal attacks are done by compromised nodes which are part of the domain network. Apart from the above mentioned attacks, MANET also faces other attacks such as Distributed Denial of Service(DDoS), Location disclosure attack, Gray hole attack, etc.

III. DISTRIBUTED DENIAL OF SERVICE (DDOS)

Denial of Service (DoS) is a type of cyber attack in which the attacker intends to make the network resource or server busy and therefore unavailable to the actual intended user. This is usually done by flooding the server or network

with unwanted false requests which overloads the systems and makes it unavailable for use by legitimate users. Distributed Denial of Service (DDoS) is an attack similar to DoS where instead of a single source flooding the network, multiple sources are involved. It is therefore difficult to stop the flooding by identifying and blocking a single source. It is basically a large scale DoS attack which poses the challenge of distinguishing between the user traffic and attack traffic.

IV. RELATED WORK

The random dynamic nature of an ad hoc networkis the main featurewhich makes it more vvulnerable to wireless attacks & congestion problem. Ad hoc nodes are independent and wireless in nature. Each node in a MANET is free to move randomly in any direction, and will therefore change its links to other nodes frequently. Each of the node is required to forward the data traffic unrelated to itself, to the neighbouring nodes. To detect the misbehaving node, the following two techniques are used : 2ACK technique and principle of conservation of flow (PFC) technique. The problem with the 2ACK algorithm is that it can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link is misbehaving. It is also difficult to identify the accurate selfish node present in the network infrastructure. Another problem in MANET is that it will drop more packets while forwarding them which leads to reduced delivery ratio, as well as lesser throughput.

V. PROPOSED WORK

Mobile ad hoc network (MANET) relies on the cooperative nature of all the participating nodes in the network. The higher the cooperation between the nodes to transfer traffic, the more stronger the network gets. Here the AODV protocol is used for route discovery, only on demand. This results in a low overhead.In order to prevent malicious users from providing fake data transmission, the packet size and packet delivery ratio is calculated.Path Tracing algorithm is used to detect the malicious attack using per hop distance and frequent appearance count parameters (pixel wisemeasurements) using AODV. Hence, we can detect the accurate misbehaving or selfish node.

5.1 Module Description

- AODV Route Discovery
- Packet Dropper Detection in MANET
- Path Tracing and Log file
- Estimate packet delivery Ratio

5.2 AODV Route Discovery

A MANET is setup with a group of independent mobile nodes that communicate with each other in a wireless environment and in the absence of a fixed infrastructure. Data packets are transmitted through the network. Here Ad hoc On-Demand Distance VectorRouting (AODV) is used. It is a type ofrouting protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, i.e., it establishes a route to a destination node only on demand. On the other hand, the most common routing protocols of the Internet are proactive, i.e., they are table driven. They calculate and determine the path to each of the nodes in the network in advance. AODV eliminates the count-to-infinity problem of other distance-vector protocols by making use of sequence numbers on route updates. AODV is applicable to bothuni cast and multicast routing.

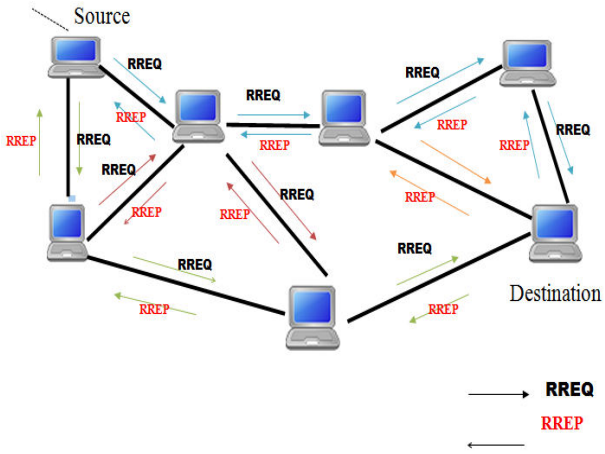

Fig.1 AODV Routing Protocol

5.3 Packet dropper Detection in MANET

Security in a MANET system can be achieved only by identifying and preventing routing protocol attacks. The malicious attack (virus, worms, etc.) is one of the challenging attacks in ad hoc network in which two malicious nodes form a tunnel with good transmission connectivity referred to as a malicious tunnel. It may be wired or wireless tunnel or an optical link. As and when the malicious nodes launch a malicious link, theybegin to gather the wireless data and forward it to each other. The real and legitimate data packets are sent to other randomlocations in the network via the malicious tunnel and the malicious nodes force the other nodes in the network to believe that they are their neighbors. In this paper, AODV is being used for route discoveryduring packet transmission and the malicious or selfish nodes are identified using the path tracing algorithm.

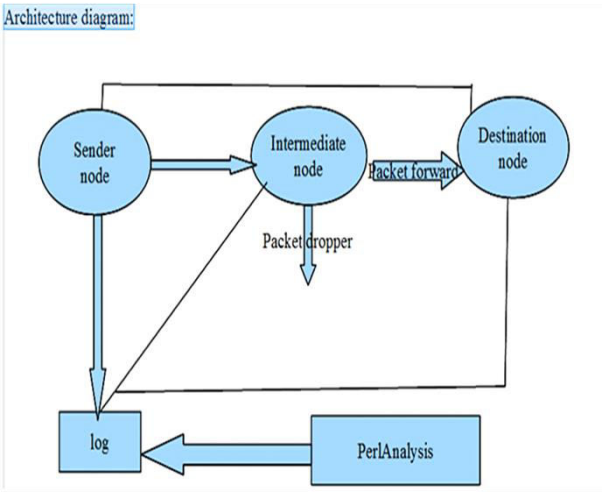

Fig.2 Packet Dropper Detection

5.4 Path Tracing Algorithm

In this paper, PT algorithm is proposed to detect and prevent wormhole attacks.

After the detection of the wormhole node it is eliminated from the network and then a fresh route is selected for the routing purpose.

As soon as the wormhole node is detected, a warning message is passed to the entire network about the presence of the wormhole node.

Therefore, all other nodes will include the ID of the wormhole attacker node in the wormhole node list.

By doing so, further attack can be prevented from the same node.

5.4 Factors of Path Tracing Technique

The wormhole is detected using the distance between per hop over a considered path. For neighboring nodes, the distance between them must be less than a predefined distance.

For calculating the per hop distance, we consider round trip time (RTT), also called round-trip delay. It is the time required for packet to travel from a specific source to a specific destination and back again.

Control packets and data packets are generally assumed to travel in the speed of light.

With these previous details, we calculate the distance per hop and store it in a DSR header. Each node calculates the per hop distance over a path in which it resides.

If per hop distance is too large or deviates from the prior per hop distance, the node may consider the corresponding node as wormhole.

In other words, when the calculated distance between them is not within the maximum acceptable transmission ranges then they are identified as wormhole nodes.

Additionally, frequent appearance count of a link in a path is considered to confirm.

VI. PER HOP ESTIMATION

The presence of malicious nodes can be detected by calculating the distance between each hop in a path. The round trip time (RTT) value is used to calculate the per hop distance. RTT is defined as RREQ and RREP propagation time between the source and destination. Consider the calculation of RTT between two nodes A and B where both are non-packet dropper nodes.

VII. VARIABLES USED IN RTT CALCULATION

T rep: Time when the first bit of RREP is received from B.

T req: Time when the last bit of RREQ is broadcasted to A.

IPD: Intra nodal processing delay

The RTT between two nodes are calculated by using formula (1)

ΔT= RTT= T rep – T req – IPD (1)

With the estimated value of ΔT, per hop distance between A and B 'DAB' is calculated assuming that routing signals travel with the speed of light 'ν'.

DAB = (ν/2) * ΔT.

DBC - DAB > R threshold

In this packet dropper is implemented using AODV routing protocol.Each node in the network has to perform four major operations to detect the packet dropper attack.Compute per hop distance and compare it with the prior per hop distance.

Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value. If it is larger, then the packet dropper is detected and it is informed to all other nodes in the network to provide packet dropper alertness. For the confirmation of packet dropper attack, the number of times a link is used in a path is also checked in addition to comparison of per hop distance. If

DBC - DAB >R threshold and

FAcount >FA threshold, then it is a packet dropper link. Per hop distance is calculated at the time of route discovery to make our proposal energy efficient.Many routes are discovered from the route discovery process. All nodes in each path calculatethe per hop distance and store in the packet header. By comparing the per hop distance between all the nodes in a path, a packet dropper can be detected. If the per hop distance exceeds the prior per hop distance by a maximum threshold range R threshold, then the path related to that particular node is packet dropper. For the effective packet dropper detection, we take another parameter called frequent appearance. If FAcount > FA threshold then it is a packet dropper link. After the detection of the packet dropper, a node intimates the presence of packet dropper to other nodes in the network.To prevent the packet dropper node participation further, their identities are added to the packet dropper list in each node. It is not necessary to compute per hop distance each time when a path is discovered. Our proposal preserves the computation energy by storing the estimated per hop distance in a cache.

VIII. ARCHITECTURE DIAGRAM

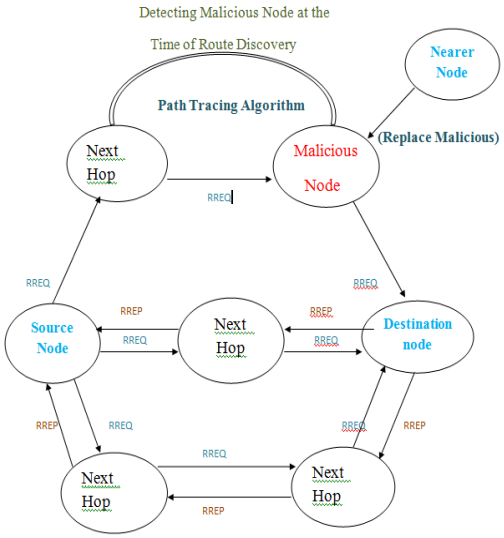

Fig3. Architecture diagram

IX. EXPERIMENTAL RESULTS

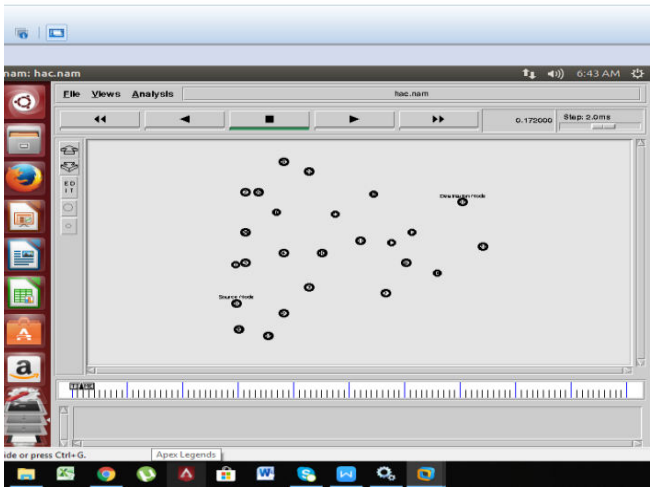

Fig4. MANET Network with Source and Destination Nodes.

Fig5. Malicious And Selfish Nodes in MANET(Marked In Red)

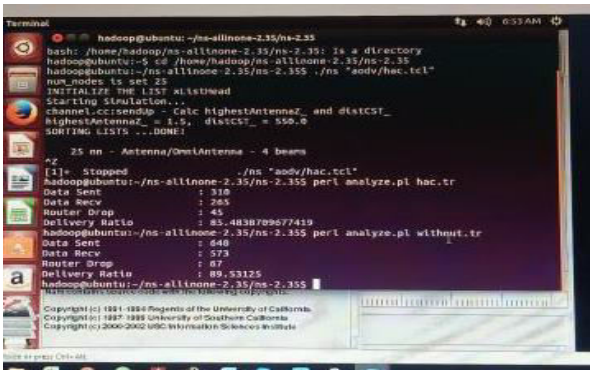

Fig6. Packet Delivery Ratio with and without Selfish node in MANET.

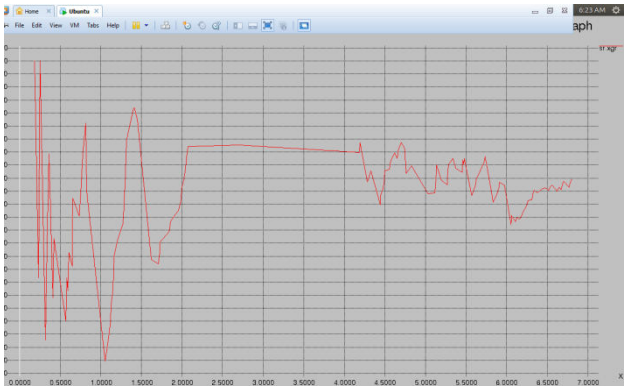

Fig7. Graph plotted by analyzing the output based on Packet Delivery Ratio (PDR) with x-axis indicating the number of nodes and y-axis indicating the time taken for the packet delivery.

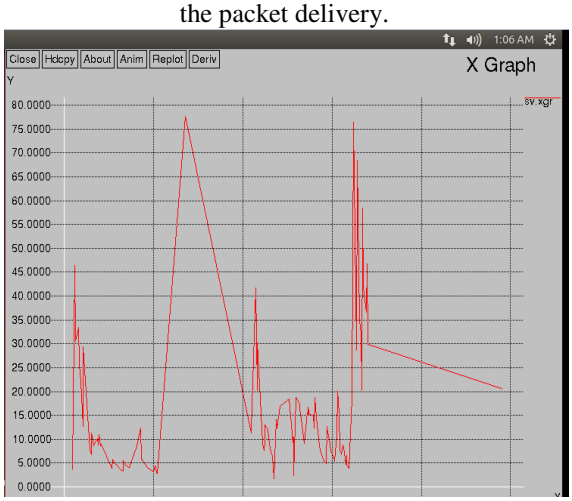

Fig8. Graph plotted by analyzing the output based on end to end delay with x-axis indicating the number of nodes and y-axis indicating the time consumed.

X. CONCLUSION

To detect and prevent the malicious attack, the proposed system uses the Path Tracing (PT) algorithm. The PT algorithm detects and prevents the malicious attack using per hop distance between two nodes. From the analysis and simulation reports, it is clear that our proposed algorithm is more effective in preventing the malicious attack with greater throughput and less average delay. The performance analysis shows that PT algorithm has reduced overhead and delay. These observations, along with the

advantage that there is no additional requirement of hardware, makes the proposed system more suitable for resource constrained, wireless network applications. Therefore, this newly proposed reputation-based strategy, built on top of normal AODV secure routing protocol, achieves a higher throughput than the normal AODV in the presence of malicious nodes. Hence, the proposed system design with reputed-AODV, proves to be more efficient and more secure than normal AODV secure routing protocol in defending against both malicious and authenticated malicious (selfish) nodes.

XI. REFERENCES

[1] Gupta, P. (2013). Detection of routing misbehavior in MANET using improved 2ACK. *IOSR Journal of Computer Engineering*, 9(1), pp.53-60.

[2] Thati, B. and Hussain, M. (2016). An Improved Dynamic Path DiscoveryAnd Selection Algorithm For Link Failure In MANET. *PONTE International Scientific Researchs Journal*, 72(12).

[3] Gonzalez et al.: Detection and Accusation of packet forwarding misbehavior in mobile ad-hoc networks, Journal of Internet Engineering, vol. 2, pp.1, 2008.

[4] Kejun Liu, Jing Deng, Pramod K. Varshney, KashyapBalakrishnan ”An acknowledgement-Based Approach for the Detection of Routing Misbehaviour in MANETs”, IEEE Transactions on Mobile Computing, vol. 6, No. 5, 2007.

[5] K.Vijaya “Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks,” TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[6] AbdelazizBabakhouya, YacineChallal, and AbdelmadjidBouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks," in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008, pp. 592-597.

[7] A book on “Security of Self-Organizing Networks: MANET, WSN, WMN, VANET”, Al-Sahib Khan Pathan

[8] SenthilkumarSubramaniyan, Wiliam Johnson, KarthikeyanSubramaniyan, EURASIP Journal on Wireless Communications and Networking 2014, https://doi.org/10.1186/1687-1499-2014-205"

[9] National Academy Science Letters, Feb 2018, Volume 41, pp 23–28, “Fuzzy based detection of malicious activity for security assessment of MANET”, DhananjayBisen and Sanjeev Sharma