ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 1, September 2014

DETECTION OF MISBEHAVIOR NODES IN MANET USING PATH TRACING ALGORITHM

A.Sathya Priya[1], Dr.Mrs.P.Krishnakumari[2]

M.Phil Research Scholar, Computer Science, RVS College of Arts & Science, Coimbatore, India[1]

Director, MCA Department, RVS College of Arts & Science, Coimbatore, India[2]

Abstract: Mobile Ad hoc Network (MANET) is an infrastructure less network. Attacks in MANET are due to unreliability, unfixed topology, limited battery power and lack of centralized control. Enhanced Adaptive Acknowledgement (EAACK) is one of the schemes used to detect misbehavior nodes in the network. It can detect the misbehaving node but cannot decide upon which one of the node associated with that link are misbehaving. It may have a chance of same misbehaving node to act as a valid route. This kind of misbehaving node is called blackhole attack. In this paper, Path Tracing Algorithm (PTA) is proposed, to find and eliminate the exact misbehaving node in network. Elliptic Curve Cryptography (ECC) algorithm is used to secure the data while passing through the network. The proposed work is simulated using NS-2 and is analyzed using certain parameters such as routing overhead, packet delivery ratio and end to end delay.

Keywords: Enhanced Adaptive ACKnowledgement (EAACK), Path Tracing Algorithm (PTA), Elliptic Curve Cryptography (ECC), DSR, Mobile Ad hoc NETwork (MANET).

I. INTRODUCTION

Mobile Adhoc Network (MANET) is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. MANET is one of the most important and unique application used for the industrial purposes. It is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. It does not require a fixed network infrastructure [1]. It can be subdivided into two types. They are single-hop and multi-hop. In single-hop networks the nodes are within communication range can communicate directly with each other. Whereas in Multi-hop networks, if the nodes are out of communicating range, the nodes must rely on intermediate nodes to forward the data packets to their destination. However, in both type of networks there is no dedicated link available like the links in wired networks. The absence of fixed and dedicated link among the nodes leads to severe security threats to the network. So an effective Intrusion Detection Scheme (IDS) is needed to safeguard the network from these threats [2], [4].

Due to the minimal configuration and quick development, MANET has been used for emergency cases. MANET are susceptible to having their effective output compromised by variety of security attacks because of features like unreliability, constantly changing topology, restricted battery power, lack of centralized control and others[3]. Nodes may misbehave either because they are malicious and deliberately wish to disturb the network or because they are selfish and wish to conserve their own limited

resources such as power. In this paper, we provide a security along with the identification of false misbehavior.

II. BACKGROUND

A. Intrusion Detection System in MANETs:

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to enhance the security level of MANETs. MANET can detect the attackers as soon as they enter the network and it is able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [5]. Existing IDS in Manets are 1) watchdog 2) TWOACK and 3) AACK.

(1) Watchdog

Marti et al. [10] proposed the Watchdog scheme, improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 1, September 2014

counter value exceeds a predefined threshold, the node is marked malicious. The major drawbacks are 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehavior report 5) partial dropping 6) collusion.

(2) TWOACK

Liu et al. [11] proposed TWOACK scheme, it overcomes the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. The major drawbacks are 1) increased overhead 2) Limited battery power 3) Degrades the life span of entire network.

(3) AACK

Sheltami et al. [12] proposed AACK scheme. Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. It reduces network overhead but fails to detect malicious nodes with false misbehavior report.

B. Digital Signature

Digital signature is a widely adopted approach to ensure the authentication, integrity, and no repudiation of MANETs. All algorithms except watchdog are based on acknowledgment. Hence, it should be authenticated through digital signature.

III. EAACK

Elhadi M. Shakshuki et al. [1] proposed EAACK scheme. Enhanced Adaptive Acknowledgment (EAACK) is designed to tackle false misbehavior, limited transmission power and receiver collision limitations of watchdog. It is capable of detecting malicious node in existance of false misbehaving report. It is an acknowledgement based Intrusion Detection System (IDS). All the Three Parts of EAACK namely ACK, S-ACK and MRA are acknowledgement based Intrusion detection system. They all rely on acknowledgement packets to detect misbehaviours in the network. If the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement packets to be digitally signed before they are sent out and verified until they are accepted.

(1) ACK

ACK is basically an end-to-end acknowledgement scheme used to reduce network overhead when no network misbehaviour is detected.

(2) S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

(3) MRA

MRA is used to detect misbehaving node with presence of false misbehaviour report. False misbehaviour report can be generated by malicious attacker to falsely report innocent node as malicious. The DSR routing finds an alternative route to transmit data through that route. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

(4) DSA and RSA

DSA always produces slightly less network overhead than RSA. The signature size of DSA is much smaller than the signature size of RSA. The Routing Overhead (RO) difference between RSA and DSA schemes vary with different numbers of malicious nodes. DSA scheme require more computational power to verify than RSA, consisting the tradeoff between battery power and performance, DSA is still preferable.

IV. PROPOSED WORK

(1) DSR

Create ad hoc networks with few numbers of nodes that communicate with each other in a wireless environment. Packets are transmitted between the nodes. In proposed Dynamic Source Routing (DSR) protocol is used. It is a reactive routing protocol that establishes a route to a destination only on-demand. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. In Route discovery phase, uses route request and route reply packets. In Route maintenance phase, uses route error packets and acknowledgments. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets. DSR does not flood the network with routing updates even when the link is not in use. A route is only determined when needed. There is no need to discover routes to all the nodes in the network. And the cached information in the intermediate nodes is used to reduce routing overhead.DSR is proposed to reduce the control traffic overhead and improve scalability.

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 1, September 2014

(2) Packet Dropper Detection

A secured MANET system can be achieved only by preventing routing protocol attacks. The malicious is one of the challenging attacks in the ad hoc routing in which two malicious nodes forms a tunnel with high transmission connectivity referred as a malicious tunnel. The malicious tunnel may be wired or wireless form or an optical link. As soon as malicious nodes launch a malicious link they start gathering the wireless data and forward it to one another. It is then relay the packets over the malicious tunnel to some other location. The legitimate data packets are relayed to some other place in the network and malicious nodes makes other nodes to believe that they are immediate neighbours. The malicious attack affects both the proactive and on demand routing protocols. In this project DSR Protocol is used to analyse its behaviour in MANET while sending packet and receiving packet to identify using path tracing.

(3) Path Tracing Algorithm

Path tracing is a computer graphics method of rendering images of three dimensionally scenes such that the global illumination is faithful to reality. Fundamentally, the algorithm is integrating over all the illuminance arriving to a single point on the surface of an object. Path Tracing (PT) algorithm, used for detection and prevention of blackhole attack is an extension of DSR protocol. The PT algorithm runs on each node in a path during the DSR route discovery process. It calculates per hop distance based on the RTT value and blackhole link using frequency appearance count. MASK is based on a special type of publickey cryptosystem. Every node in a path has to compute per hop distance of its neighbour with the previous per hop distance to identify the blackhole attack. The corresponding node detects the blackhole if per hop distance exceeds the maximum threshold range. In the routing process the blackhole link participates more than the normal link.

(4) Node deployment and packet routing

Packets are forwarded using source routing. Let us consider a group of random mobile nodes consists of a set R= {r1, r2, r3…., rn} that communicate each other using radio transmission and the neighbouring node communicate each other in a bidirectional fashion. For neighboring nodes, the distance between them must be less than a predefined distance‘d’. In this paper how the nodes make use of MAC protocol to gain access in radio transmission is not concentrated. The network is designed such that it has loose clock synchronization. All nodes in ad hoc environment may or may not be resource controlled.

(5) Blackhole attack Detection

A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it. These black hole nodes may work as a group.

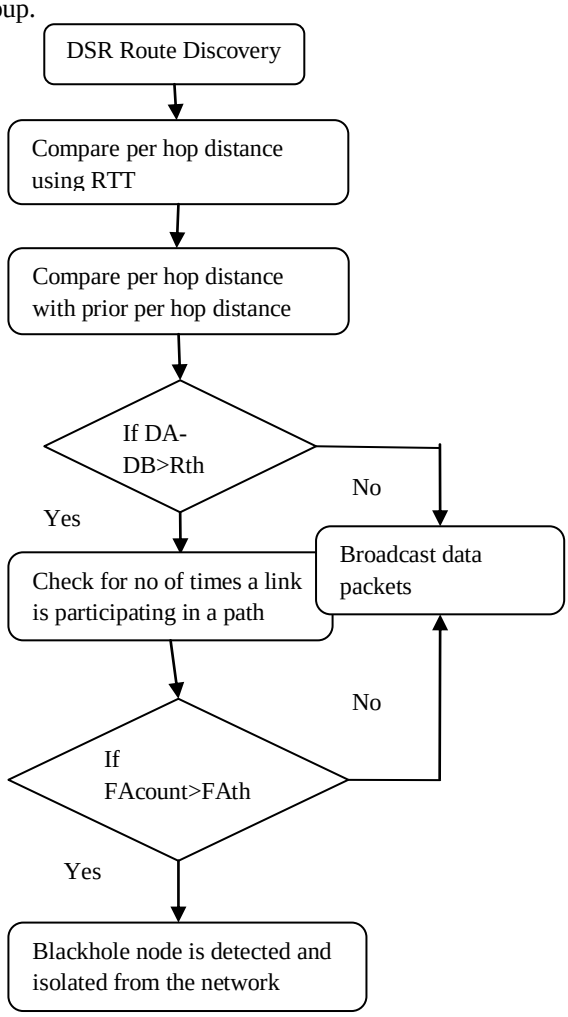

Fig 1: System architecture for Detecting Blackhole Attack

(6) Per Hop Distance Estimation

The presence of blackhole can be detected by calculating the distance between each hop in a path. Consider the round trip time (RTT) value to calculate the per hop distance. RTT is defined as RREQ and RREP propagation time between the source and destination. Examine the RTT calculation between two nodes A and B where both the nodes are non blackhole nodes. The calculation of per hop distance is performed during the route discovery process in order to reduce the routing overload. Each node must run the per hop distance calculation using RTT value and store the estimated per hop distance value in packet

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 1, September 2014

header. The blackhole can be detected using the information in the packet header.

(7) Analysis of Frequent Appearance of a link

In order to detect the blackhole attack effectively, a link can be checked whether it participates in the routing very often. Find the frequent appearance (FAcount) of a link (Lj) in a path by using the formula, FAcount = Maximum number of times that Ljparticipates in a path (Nj) / Total number of available links in a path (N). As there are many links in a path, it can also be used to detect blackhole attacks. If a link in a path frequently takes place in routing such that its count exceeds the frequent appearance threshold (FA_{Th}), then it is a blackhole link. The frequent appearance count information is gathered only through the monitoring and marked in cache. The proposal is easy to implement with reduced overhead requirements and does not rely on fixed time synchronization. Every node must calculate RTT only using its own clock.

(8) Steps to detect blackhole attacks

Step 1: Nodes in a path computes RTT values based on the time between the RREQ sent and RREP received. The RTT computation is based on its own clock.
Step 2: Compute per hop distance value using RTT value. The computed per hop distance value and timestamp are stored in each packet header.
Step 3: These informations are stored to identify the blackhole link. Every node in a path computes per hop distance with its neighbor and compares it with the prior per hop distance. If the per hop distance exceeds the maximum threshold range, R_{Th}, go to step 4.
Step 4: Check for the maximum count a link takes part in the path. If FAcount> FATh, then the link is blackhole.
Step 5: Mark the link as blackhole and the corresponding node informs other nodes to alert the network. These blackhole nodes are then isolated from the network.

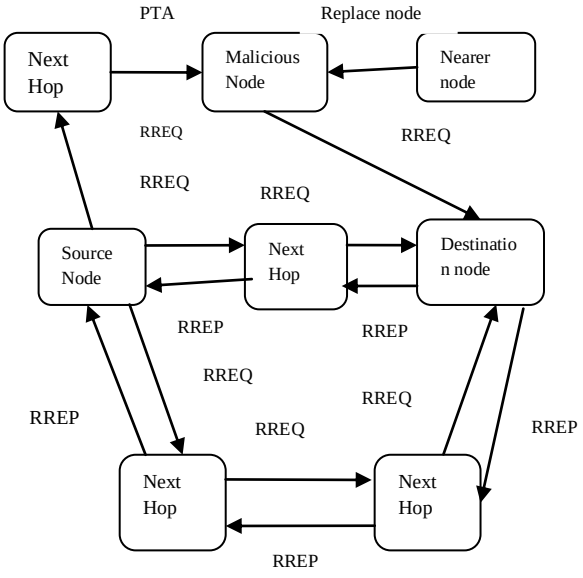

Fig 2: Detecing Malicious node at the time of routing

(9) Elliptic Curve Cryptography Cryptography(ECC) algorithm

Elliptic curve Cryptography (ECC) algorithm is used to enhance the security in Ad-hoc wireless network. ECC algorithm is being used for encryption and decryption. Communication is secured as the data cannot be viewed while passing through the network.

V. SIMULATION PARAMETERS

In this section, the simulation environment and the simulation results are discussed. Simulation is done using the network simulator NS-2. The numbers of nodes we have considered for simulation are 10 to 50 mobile nodes in the terrain area of 1000m *1000m.The traffic model chosen is CBR (Constant Bit Rate) connections with packet size of 1000 bytes to emulate traffic over the network. Each node independently repeats this behavior and mobility is varied by making each node stationary for a period of pause time. The packets are routed using Dynamic Source Routing (DSR) protocol and the acknowledgements are authenticated using Elliptic Curve Cryptography.

Table 1: Simulation parameters

Parameter Name	Parameter Value
Simulation tool	NS-2
Simulation area	1000x1000
Number of nodes	50
Mobility speed	5ms
Maximum packets in interference queue	250
Antenna	Omni directional
Traffic model	Constant Bit Rate(CBR)
Communication Agent	TCP
Packet size	1000 bytes
Routing protocol	DSR

V. PERFORMANCE EVALUATION

The metrics used in evaluating the performance are:

(1) Packet Delivery Ratio

It is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes. It can be defined as: PDR = total no. of packet received / total no. of packet send

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 1, September 2014

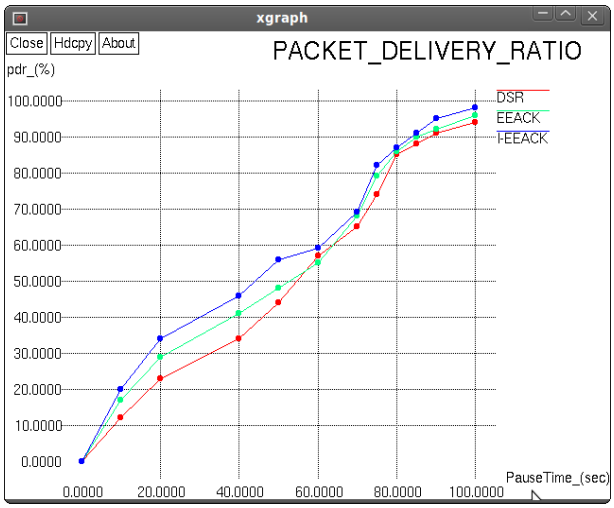

Fig 3: Performance analysis on PDR

(2) End-to-End delay

This is average delay between the sending of packets by the source and its receipt by the receiver. It means it is difference between the receiving time and sending time. This includes all possible delays caused by buffering during data acquisition, route discovery, queuing, processing at intermediate nodes, retransmission delays, propagation time, etc. It can be defined as: Avg. D=S/N Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

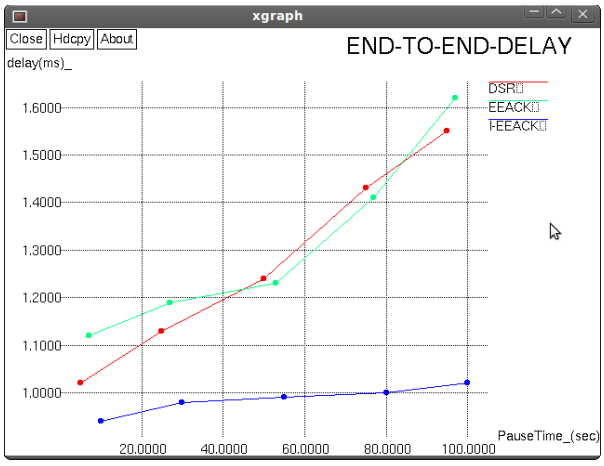

Fig 4: Performance analysis on delay

(3) Routing Overhead

Routing overhead refers to the ratio of routing related transmissions. The control overhead is defined as the total number of routing control packets normalized / the total number of received data packets

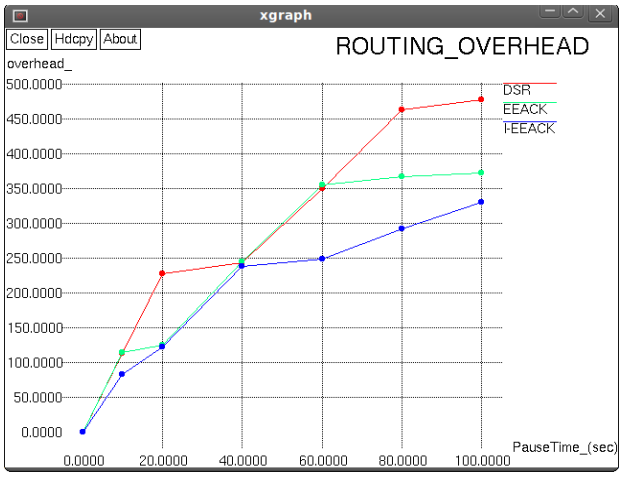

Fig 5: Performance analysis on Routing overhead

VII. CONCLUSION

Packet dropping attack has always been a major threat to the security in MANETs. The blackhole or packet drop attack which is one of the network layer attacks. This kind of attacker launches attacks by forming a channel between two or more malicious nodes and drops all the packets. To detect and prevent the blackhole attack, Path Tracing (PT) algorithm has been proposed. The PT algorithm detects and prevents the blackhole attack using per hop distance between two nodes. It depends on DSR protocol. ECC offers strong privacy protection, complete unlinkability and content unobservability for ad hoc networks. The security analysis demonstrates that ECC not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The proposed work is simulated using NS-2. The performance analysis addresses that PT algorithm has reduced the overhead and delay and increases the packet delivery ratio of the network. Blackhole attack can also implemented by using AODV protocol in future.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami,"EAACK—A Secure Intrusion-Detection System for MANETs", *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS*, VOL. 60, NO.3, MARCH 2013.

[2] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. *IEEE Int. Conf.Perform., Comput, Commun*, 2004, pp. 747–752.

[3] R. Praveen Kumar, A.Excellencia, P.Kanimozhi, "Providing a New EAACK to Secure Data in MANET", *IJREAT*, Volume 2, Issue 2, ISSN: 2320 – 8791

[4] S. Sanjith ,M. Padmadas , and N. Krishnan, "EAACK – Based Intrusion Detection and Prevention for MANETs using ECC Approach", *IJETTCS*, Volume 2, Issue 4, July – August 2013

[5] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[6] Ipsita Panda," A Survey on Routing Protocols of MANETs by Using QoS Metrics", *International Journal of Advanced Research in Computer Science and Software Engineering 2* (10), October-2012, pp. 120-129

[7] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET", (IJCNWC), ISSN: 2250-3501 Vol.2, No5, and October 2012.

[8] R. Vembu, R. Syed hayath," Methodology For Comparing Reactive Routing Protocols To Detect And Prevent The Wormhole

Attcak Using Path Tracing Approach", (IOSR-JECE) E-ISSN: 2278-2834, P-ISSN: 2278-8735 PP 12-17

[9] M.Ponnrajakumari, Abirami.S.P, Kalyani.R, Subhashri.M, Suchithra.R, "A Secure Intrusion Detection Using Improved EAACK in Manets", *IRF International Conference, Chennai,* 23rd March. 2014, ISBN: 978-93-82702-67-2

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc.6th Annu. Int. Conf. Mobile Comput. Netw, Boston, sssMA, 2000, pp. 255–265.

[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[12] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.