IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
**ISSN: 2320 – 8791 (Impact Factor: 1.479)**
**www.ijreat.org**

# Providing a New EAACK to Secure Data in MANET

**Mr. R. Praveen Kumar[1], A.Excellencia[2], P.Kanimozhi[3]**

[1]**Assistant Professor, Department of Information Technology, Anand Institute of Higher Technology, Chennai.**

[2,3]**UG Student, Department of Information Technology, Anand Institute of Higher Technology, Chennai.**

**ABSTRACT**

Effective network security targets a variety of threats and stops them from entering or spreading on a network. Mobile Ad hoc NETwork (MANET) is a infrastructure less network. Attacks in MANET are due to unreliability , unfixed topology, limited battery power and lack of centralised control. Enhanced Adaptive ACKnowledgement (EAACK) is used to detect misbehaviour in network. 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. This technique will not give more security. This limitation is been overcomed in this paper. Path Tracing Algorithm (PTA) is used to find the exact misbehaving node. Elliptic Curve Cryptography (ECC) algorithm is used to secure the data while passing through the network.

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

## 1 .INTRODUCTION

Due to their mobility and scalability the wireless networks are used to extend according to their frequency range. Owing to the proposed technology and reduced cost, wireless networks have gained much more preferences over wired networks. Mobile Ad hoc NETwork (MANET) is one of the most important and unique application used for industrial purposes [2], [4]. It is a collection of nodes where both the transmitter and receiver that communicate with each other through bidirectional wireless links either directly or indirectly. It does not require a fixed network infrastructure [3]. It can be subdivided into two types. They are single-hop and multi-hop. One of the advantages of wireless network is that it has the ability to allow data between different nodes and still maintain their mobility. If the two nodes are beyond their communication range then it is not possible for them to send the data in a single-hop network. Whereas in multi-hop network we use an intermediate node to transfer data from source node to destination node even if they are not within the communication range. Due to their minimal configuration and quick development we use MANET 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. 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. The purpose of this project is to provide security along with identification of false misbehaving. The Path Tracing Algorithm (PTA) is used to detect and prevent the malicious node. Elliptic Curve Cryptography (ECC) algorithm is used to provide security to the data that is sent between the nodes.

## 2. RELATED WORKS

2.1Watchdog -Watchdog reports in misbehaving and improve throughput of network with presence of malicious node [5], [8]. Watchdog fails to detect malicious misbehaviours with the presence of 1)ambiguous collision; 2)receiver collision; 3)limited transmission power; 4)false misbehaving report; 5)collusion and partial dropping [7].

2.2 TWOACK- Used to resolve receiver collision and limited transmission power of watchdog.

2.3 AACK- It is a combination of TWOACK and end-to-end ACKnowledgement (ACK) scheme. It reduce network overhead.

## 3. EAACK DESCRIPTION

3.1 EAACK- Used to detect misbehaviour in the network. It is a combination of ACK, Secure ACK (SACK) and Misbehaviour Report Authentication (MRA). 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 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.

3.2 ACK- It is a end-to-end acknowledgement scheme used to reduce network overhead when no network misbehaviour is detected.

3.3 S-ACK- It is a version of TWOACK. It is used to detect misbehaving node in presence of receiver collision and limited transmission power [6].

3.4 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.

3.5 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.

## 4. PROPOSED WORK

4.1AODV Route Discovery- Create ad hoc networks with few number of nodes that communicate with each other in a wireless environment. Packets are transmitted between the nodes. We are using Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AODV is capable of both unicast and multicast routing.

4.2 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 AODV Protocol is used to analyse its behaviour in MANET while sending packet and receiving packet to identify using path tracing.

4.3 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 for detection and prevention of wormhole attack as an extension of AODV protocol. The PT algorithm runs on each node in a path during the AODV route discovery process. It calculates per hop distance based on the RTT value and wormhole link using frequency appearance count. MASK is based on a special type of public-key cryptosystem. Every node in a path has to compute per hop distance of its neighbour with the previous per hop distance to identify the wormhole attack. The corresponding node detects the wormhole if per hop distance exceeds the maximum threshold range. In the routing process the wormhole link participates more than the normal link.

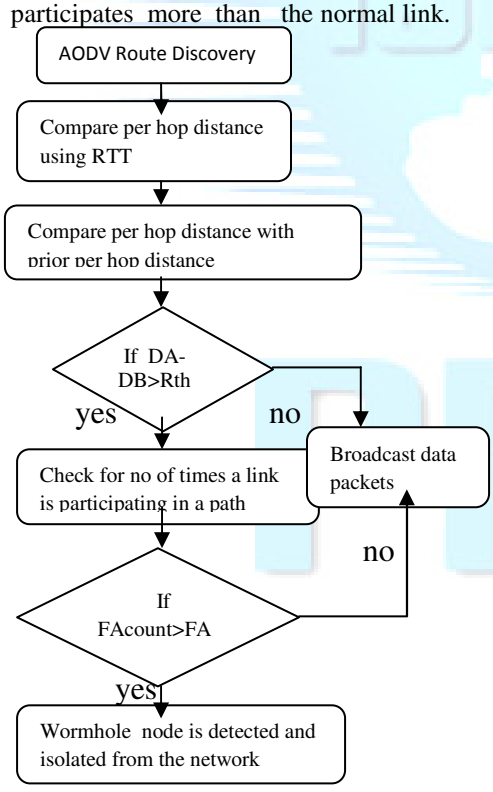


Fig.1. System Architecture for Detecting Wormhole Attack

4.4 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.

4.5 Wormhole Attack Detection-The source node floods the route request (RREQ) packets through immediate neighbors towards destination. When it reaches the destination, it sends back route reply (RREP) in the reverse path. The path details are stored in the AODV routing cache. In order to detect the wormhole, we optimize the general DSR header by adding extra fields. Prior per hop distance field, per hop distance field and timestamp fields are added to the header of each packet. We consider both prior per hop distance and per hop distance so as to compare the difference between the two distances. If the difference is too large that exceeds the maximum threshold value, then wormhole is detected. All nodes that participate in the routing mechanism perform this operation.

4.6 Per Hop Distance Estimation -The presence of wormhole can be detected by calculating the distance between each hop in a path. We consider 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. Let us consider the RTT calculation between two nodes A and B where both the nodes are non wormhole 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 header. The wormhole can be detected using the information in the packet header.

4.7 Analysis of Frequent Appearance of a link-In order to detect the wormhole attack effectively, a link can be checked whether it participates in the routing very often. We can find 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 wormhole attacks. If a link in a path frequently takes place in routing such that its count exceeds the frequent appearance threshold (FATh), then it is a wormhole link. The frequent appearance count information is gathered only through the monitoring and marked in cache. Our proposal is easy to implement with reduced overhead and requirements and does not rely on tight time synchronization. Every node must calculate RTT only using its own clock.

4.8 Packet Delivery Ratio and throughput- PDR is the proportion of the total amount of packets reached the receiver and amount of packet sent by the source. If the amount of malicious node increases, PDR also decreases gradually. The higher mobility of nodes causes PDR to decrease. The network throughput for the different percentage of nodes. The throughput decreases as the amount of malevolent nodes increase PDR = Total amount of data packet received (Receiver) /Total amount of packet sent (Source).

4.9 Steps to detect the wormhole 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 wormhole 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, RTh, 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 wormhole.

**Step 5:** Mark the link as wormhole and the corresponding node informs other nodes to alert the network. These wormhole nodes are then isolated from the network.

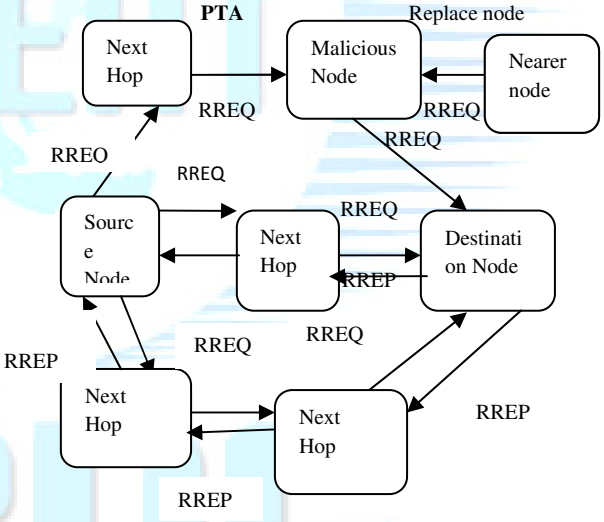


Fig.2. Detecting Malicious node at the time of routing

4.10 ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

In this paper 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.

## 5. CONCLUSION

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. In this paper we implemented the protocol on ns2 and examined performance of ECC, which shows that ECC has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes. Wormhole attack cannot be prevented with DSR protocol so we propose AODV protocol for detecting and preventing of wormhole attack using path tracing approach.

## REFERENCES

[1] Ellade M.Shakshuki, Senior member, Nan Kang, and Tarek R.Sheltami, "EAACK-a secure intrusion detection system for MANETS" IEEE trans on industrial electronics, vol.60, No.3, March 2013.

[2] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technology," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct.2009.

[3] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[4] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4,pp. 1835–1841, Apr. 2008.

[5] 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.

[6] 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.

[7] 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.

[8] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.