ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 4, April 2014

Adopting a key Exchange Mechanism to Eliminate the Requirements of Pre-distributed key in MANET

N.Arunmani[1], S.Kannan[2], S.Karthik[3]

[1]PG Scholar, [2]Assistent professor of CSE, [3]DEAN and Professor of CSE
Department of Computer Science and Engineering,
SNS College of Technology, Coimbatore-641035.

***Abstract*- MANET is a collection of mobile nodes and it is an infrastructure less wireless mobile network. They have a highly dynamic topology with nodes having a transceiver to send and receive data. It is a self-configuring network of mobile routers connected by wireless links. Network is an autonomous transitory association of mobile nodes which communicate directly with each other and are responsible for dynamically discovering each other. Some of the issues in MANET are Routing, Security and Reliability, Quality of Service, Power Consumption, Packet Transmission, Bandwidth, Data Caching, Replication, Lack of centralized Management and Resource Availability. Security is a paramount concern in MANET because of its intrinsic vulnerabilities. By the survey made in different papers, the improvements of technology and cut in hardware costs is a current trend of expanding MANETs into industrial application.It is witnessed that to adjust to such a trend it should be strongly believed that it is vital to address its security issues. Packet dropping attack is always being a major threat to the security in MANET. So novel IDS named EAACK protocol is designed, but the result demonstrated that protocol performed poorly due to receiver collision, limited transmission power, and false misbehavior report,improved results are obtained by using DSA and RSA algorithms. With the help of hybrid cryptographic techniques like Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) there is a possibility of reducing the network overhead.**

***Keywords*- Packet dropping, Misbehavior report, MANET**

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a self-creating, self-organizing and self-administering wireless network. MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links.The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. It is a self-configuring network of mobile nodes connected by wire-less links the union of which forms an arbitrary topology. The nodes are free to move randomly and organize themselves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably.Each node in a MANET acts as a router, and communicates with each other.

A large variety of MANET applications have been developed. For example, a MANET can be used in special situations, where installing infrastructure may be difficult, or even infeasible, such as a battlefield or a disaster area.Such networks are aimed to provide communication capabilities to areas where limited or no communication infrastructures exist.Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. Message routing is a problem in a decentralize environment where the topology fluctuates.

That is here nodes within each other's radio range communicate directly via wireless links while those are far apart uses other nodes as relays. This kind of network is well suited for the mission critical applications such as emergency relief, military operations where no pre-deployed infrastructure exists for communication.

Due to the lack of authorization facilities, volatile network topology it is hard to detect malicious nodes, MANETs are highly vulnerable to attacks.

Finally, in MANET nodes might be battery-powered and might have very limited resources, which may make the use of heavy-weight security solutions undesirable. Many different types of attacks have been identified.In such a network, each node not only plays the role of an end system, but also acts as a router that forwards packets to desired destination nodes. These nodes are capable of both single and multi-hop communication. Mobility and the absence of any fixed infrastructure make MANETs very attractive for military and rescue operations, sensor networks and time-critical applications. It deals with the Denial of service attack (DoS) by a selfish node; this is the most common form of attack which decreases the network performance.

The nodes in a MANET in order to keep up the fairness of distribution in the network 'channel' are expected to wait for a pre specified period of time between successive transmissions.As one might expect the MANET is a self-made network without any arbitrator to chastise nodes which fails to follow the protocols. A node might choose non-random and t back off value in order to transmit more frequently. This will on one hand enable that node to more effectively, utilize the channel and improve its throughput.

II.REALTED WORK

Since prevention techniques are never enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms. Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Conventional IDSs are not easily applied to them. New approaches need to be developed or else existingapproaches need to be adapted for MANETs. Survey outlines issues of intrusion detection for MANETs and reviews the main solutions.[1]

A malicious node falsely reports other nodes as misbehaving while in fact it is the true culprit. Each node maintains a table that records the number of packets the node sends forwards or receives respectively. When receives a report about misbehaving nodes, the source of a communication can send a message to the destination to check if the sums of packets the two parts stores are equal. If they are equal, then the real malicious node is the node that reports others nodes as misbehaving. Otherwise, nodes being reported malicious do misbehave.[5]

One of the major sources of energy consumption in mobile nodes of MANETs is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.The 2ACK scheme to mitigate the adverse effects of misbehaving nodes.

The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. Such a 2ACKtransmission takes place only for a fraction of data packets, but not all. Such a selective acknowledgment1 is intended to reduce the additional routing overhead caused by the 2ACK scheme. [3]

The more nodes that participate in packet routing, the greater the aggregate bandwidth, the shorter the possible routing paths, and the smaller the possibility of a network partition. However, a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious, or broken. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets.

A selfish node is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets.

Explores a different approach and installs extra facilities in the network to detect and mitigate routing misbehavior. In this way, we can make only minimal changes to the underlying routing algorithm. We introduce two extensions to the Dynamic Source Routing algorithm (DSR) to mitigate the effects of routing misbehavior.When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by Listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving. The path rater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets.[4]

To the best of our knowledge, this IDS is the first actual implementation deployed on handheld devices..it also describe the implementation of our secure routing protocol, SecAODV.It also provides detailed analysis of issues involved in the implementation and deployment of a secure routing protocol and IDS. SecAODV and the snooping IDS complement each other in being able to detect most of the prevalent attacks.The goal is to detect malicious or chronically faulty nodes and deny them network resources.[6]

A counter is maintained which is incremented every time node misconduct is detected, subsequently after a particular value is cross the node is labeled as misbehaving and the information is broadcast over the network. Results: Performance parameters like throughput, packet delivery ratio were monitored with traffic of the magnitude 10 to 60 nodes. Also the performance of the network based on the percentage of selfish nodes present in the network was monitored and a graph was generated based on the statistics.[4]

Analysis discuss about the main problem of any public-key based security system is to make each user's public key available to others in such a way that its authenticity is verifiable More precisely, two users willing to authenticate each other are likely to have access only to a subset of nodes of the network. The best known approach to the public-key management problem is based on public-key certificates.

A public-key certificate is a data structure in which a public key is bound to an identity (and possibly to some other attributes) by the digital signature of the issuer of the certificate.In PGP, user must create the public and private keys themselves. Certificates system are stored and distributed by the nodes in a fully self-organized manner. Each certificate is issued with a limited validity period and therefore contains its issuing and expiration times. Before a certificate expires, its issuer issues an updated version of the same certificate, which contains an extended expiration time.[1]

III. METHODOLOGY

The EAACK scheme was extended with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA). In order to distinguish different packet types in different schemes, they included a two-bit packet header in EAACK.

According to the Internet draft of DSR, there are six bits reserved in DSR header. In EAACK, two of the six bits were used to flag different type of packets. In the proposed scheme it was assumed that the link between each node in the network is bi-directional.

Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.

EACCK mechanism depends only on ACK and chances to make

false acknowledgement.DSR based on source routing mechanism, if any link failure occurs in the network, DSR send a unicast packet to the source giving the information about the broken link but source may change dynamically. DSR has more routing overhead, less frequent route discovery and E2E delay.Increase in network overhead.Requirement of predistributed keys.

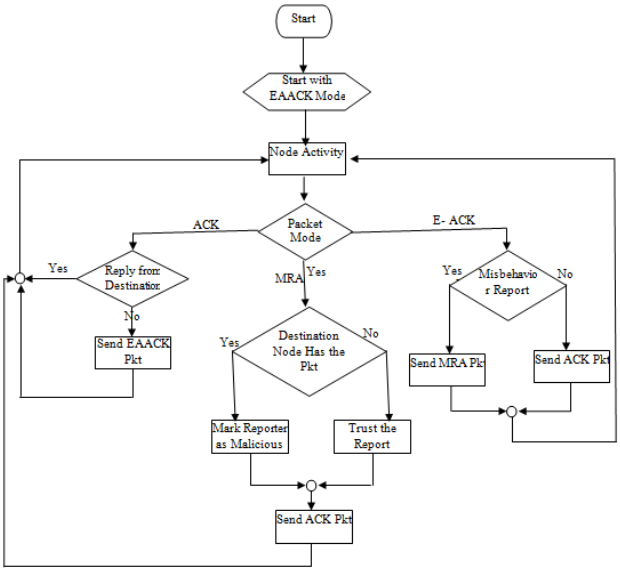

Fig. 1 EAACK Scheme

A. ACK

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected.Within a predefined time period, if node S receives ak1 P, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

B. S-ACK

The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

C. MRA

The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. DSA requires more battery power than RSA.Considering the tradeoff between battery power and performance, DSAis still preferable.

D. AES and SHA

In order to reduce the network overhead and provide security we use two methods AES and SHA.AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a feistel network. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. SHA(secure hash function) used to convert the message to a unique representation of the messagewithout loss of information about its exact original length add as many zeroes as necessary to reach the target length,. Finally, append the original length of the message.

IV CONCLUSION

The analysis designed an attack detection system called the EACK IDS, featuring active response capabilities. Through the incorporation of principles pertaining to attack Encryption algorithm, the AES. This system described a secure based EACK intrusion detection approach in MANET. This approach is simple but it requires monitoring many features. We apply AES in our feature selection and found that the algorithm is accurate by verifying. The proposed EACK with AES with ECC elipitical curve cryptograpry we can able to reduce the network overhead outperforms then all other schemes and capable of detecting false misbehavior nodes and produce the report. Experimental studies have shown that algorithm can decrease the number attacks and features dramatically with very similar detection rate.

REFERENCES

[1] Capkun.S, Buttyan.L, and Hubaux.J, (2007)"Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput, vol. 2, no. 1, pp. 52–64.

[2] Kang.N, Shakshuki.E, and Sheltami.T,(2010) "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France,vol. 8,no .8, pp. 216–222.

[3] Liu.K, DengJ, Varshney.P.K, and Balakrishnan.K,(2007) "An Acknowledgment based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–55

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

[5] Naser.N and Chen.Y(2007) "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in MANET "in proc.IEEEint.conf.commun.,Glasgow,Scotland, vol 147 no.18 pp .384-387.

[6] Parwardhan.A, Pinkston.J, and Joshi.A and T.Karygianis,(2005) "Secure Routing and intrusion detection System in adhoc networks"3rdInt.Conf. Pervasive Comput.Commun.,vol .47 no .7 pp-191-199.