Abstract

There are many methods presented in literature to secure the routing in MANET. However these methods suffered from different kinds of limitations. In this project we are investigating and extending recently presented method called EAACK with aim of reducing the network overhead while improving the malicious node detection rate. In this project we are employing the new hybrid cryptography algorithm in EAACK rather than using digital signature. This new method we can called as Improved EAACK..

Keywords: ACK, EAACK, IEAACK, MANET etc

1. INTRODUCTION

In Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. There is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium.

MANET

MANET 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. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

Fig 1 Architecture of MANET

2. LITERATURE SURVEY

Elhjadi M. Shakshuki, Nan Kang and Tarek R. Sheltami[1].The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications[1].

G. Jayakumar and G Gopinathmk Mobile ad hoc networks(MANET) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self organize into arbitrary and tempor ary
adhoc network topologies, allowing people and devices to seamlessly internet work in areas with no preexisting communication infrastructure e.g., disaster recovery environments.\[2\]  
N. Nasser and Y. Chen As mobile wireless ad hoc networks have different characteristics from wired networks and even from standard wireless networks, there are new challenges related to security issues that need to be addressed. Many intrusion detection systems have been proposed and most of them are tightly related to routing protocols, such as Watchdog/Pathrater and Routeguard. These solutions include two parts: intrusion detection (Watchdog) and response (Pathrater and Routeguard).\[3\]

Security Attacks in MANET The present attacks on MANET highly concentrated around DoS. The different types of attacks are listed in Table 1

<table>
<thead>
<tr>
<th>Layers</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Repudiation, data corruption</td>
</tr>
<tr>
<td>Transport</td>
<td>Flooding</td>
</tr>
<tr>
<td>Network</td>
<td>Worm hole, Black hole</td>
</tr>
<tr>
<td>Data link</td>
<td>Traffic analysis</td>
</tr>
<tr>
<td>Physical</td>
<td>Eavesdropping, Jamming</td>
</tr>
<tr>
<td>All</td>
<td>DoS</td>
</tr>
</tbody>
</table>

**Flooding Attack**
The malicious node which is may be or may not be a part of a MANET may send huge number of request packets to a node which is part of the network and thus may disrupt the availability of the service of the victim node. This attack is a form of denial of service attack. Fig.2 represents flooding attack.

**Worm hole**
In this attack intruders are more than one with a high speed link in use. Requests go through the attacker zone to the destination using the high speed link. Destination confirms this false high speed link as an optimum route and replies back. As a result, all data transmission is open to the malicious nodes. Fig.2.2 represents a schematic diagram for worm hole attack.

**Black hole**
The entire data pass through the malicious node as it claims itself to be the optimum route by fabricating the sequence number in packets higher than the other nodes and sends fake reply to the source. Fig.2.3 represents black hole attack.

**Traffic analysis**
The intruder attempts to guess the traffic being transmitted between the sender and receiver. It is a passive attack which is difficult to detect but easy to defense by implementing required encryption technique. Fig.2.4 represents traffic analysis scheme.

**Eavesdropping**
Eavesdropping attack in MANET shares the wireless medium, as wireless medium make it more vulnerable for MANET malicious nodes to intercept. The attacker node intercepts the transmission as every MANET node is equipped with transceiver in range of the communication which can be decode by means of malicious node to target the authorized node on the network, malicious node can obtain the sensitive information etc. modify the routing route or poison the routing table.

**Jamming**
Jamming is one of many exploits used compromise the wireless environment like MANET. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. Jamming can result in denial of service attack.

**Denial of Service**
It is an extended version of jamming attack. It can occur in any layer. Denial of Service refers to the situation where a service is made unavailable to the legitimate users by sending huge number of requests to the service at a time EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [4], there is 6 b reserved in the DSR header. In
EAACK, we use 2 b of the 6 b to flag different types of packets.

**PROBLEM STATEMENT**

**A. ACK**

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node S first sends out an ACK data packet Pa[d]1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pa[d]1, node D is required to send back an ACK acknowledgment packet Pa[k]1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pa[k]1, 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[5].

**B. S-ACK**

The S-ACK scheme is an improved version of the TWOACK scheme proposed. 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. In S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet Psad1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S[6].

**C. MRA**

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs.

**D. Digital Signature**

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA [33] and RSA [4] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

**EXISTING SYSTEM**

Many routing protocols are introduced for the wireless communication network by conducting various researches over those routing protocols, however such routing protocols having the problems of dependency over the mobile nodes majorly for the operation of routing and hosting for data sending. Every routing protocol is trusting over all the mobile nodes in networks for proper working. Mobile networks are open in nature and hence this is resulted into different kinds of network attacks which are happening due to such mobile nodes in the network. Mobile ad hoc network is threaten to various kinds of network attacks such as Denial of Service Attacks, Gray hole attacks, black hole attacks, worm hole attacks etc. This all attacks are possible only because of the mobile nodes in the MANET those are acting as misbehaving nodes in the network. In the literature we have studied four recent methods such as watchdog, TWOACK, AACk, EAACK for efficient detection of malicious uses in MANET. However each of this method suffered from different limitations and problems.

**Goals**

- To present literature review different methods EAACK - Intrusion Detection System for MANET
- In this research work, our goal is to propose a new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem.

**Objectives**

The wireless network has ability to allow data communication in different parties along with providing its mobility nature. But this communication is limited to a specific range. To solve this problem MANET is used. MANET divides network into two parts, such as single hop, and multi-hop [1]. In single-hop all nodes within the
same mobile range can communicate directly with each other and in multi-hop MANET network, the mobile node can use the intermediate nodes for transmission of information from source to destination.

**Scope**

ACK is an end to end acknowledgement based scheme. It acts as a part of the hybrid scheme in EAACK, which aims to reduce network overhead when no network misbehavior is detected. When an acknowledgement from source to destination doesn’t reach in a specific period of time then source will automatically switches to the next scheme i.e. S-ACK mode

**Proposed System**

**Fig.2:** Proposed System Architecture

- **Current node:** If an attacker sends any packet to gather information through this system, Home agent calls the classifier construction to find out the attacks. If an attack has been occurred, it will filter the respective system from the global networks.
- **Home agent:** It is present in every system and it collects information about its system from application layer to network layer.
- **Neighboring node:** In this any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message it send mobile agent to the neighboring node.
- **Data collection:** This module is used for each anomaly detection subsystem to collect the values of features for corresponding layer in a system. Normal profile is created using the data collected during the normal scenario and attack data is collected during the attack scenario.
- **Data process:** Data preprocessing is a technique to process the information with the test train data. The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. In the entire layer anomaly detection system, the above mentioned preprocessing technique is used.
- **Local integration:** This module concentrate on self system and it find out the local anomaly attacks. Every system under that wireless network follows the same methodology to provide a secure global network.
- **Global integration:** Global integration module is used to find the intrusion result for entire network. The aim of this module is to consider the neighbor node(s) result for taking decision towards response module.

**ALGORITHM**

**DIGITAL SIGNATURE ALGORITHM (DSA)**

**RSA Algorithm**

The RSA algorithm is used for both public key encryption and digital signatures. It is the most widely used public key encryption algorithm. The basis of the security of the RSA algorithm is that it is mathematically infeasible to factor sufficiently large integers. The RSA algorithm is believed to be secure if its keys have a length of at least 1024-bits.

**Key Generation Algorithm**

1. Choose two very large random prime integers: p and q
2. Compute n and φ(n): n = pq and φ(n) = (p−1)(q−1)
3. Choose an integer e, 1 < e < φ(n) such that: gcd(e, φ(n)) = 1
4. Compute d, 1 < d < φ(n) such that: ed = 1 (mod φ(n))

**Generation of Prime p and q**

- **p = a prime modulus, where 2^{159} < p < 2^{160} for 512 ≤ L ≤ 1024 and L is a multiple of 64. So L will be one member of the set {512, 576, 640, 704, 768, 832, 896, 960, 1024}**
- **q = a prime divisor of p-1, where 2^{159} < q < 2^{160}**

**Generation of Prime p and q**

The generation is hard to understand but I found a good description of it...

The prime generation scheme starts by using the SHA and a user supplied SEED to construct a prime, q, in the range 2^{159} < q < 2^{160}. Once this is accomplished, the same SEED value is used to construct an X in the range 2^{159} < X < 2^{160}. The prime, p, is then formed by rounding X to a number congruent to 1 mod 2q as described below. An integer x in the range 0 ≤ x < 2^a may be converted to a g-long sequence of bits by using its binary expansion as shown below:

```
x = x_1* 2^a + x_2* 2^(a-1) + ... + x_a* 2^0
```

Conversely, a g-long sequence of bits \{ x_1, ..., x_g \} is converted to an integer by the rule:

```
x = x_1* 2^a + x_2* 2^(a-1) + ... + x_g* 2^0
```

Note that the first bit of a sequence corresponds to the most significant bit of the corresponding integer and the last bit to the least significant bit. Let L = 1 = n* 160 + b, where both b and n are integers and 0 ≤ b < 160.

**Step1.** Choose an arbitrary sequence of at least 160 bits and call it SEED. Let g be the length of SEED in bits.

**Step2.** Compute
Before getting the digitally signed message the receiver must know the parameters \( p, q, g, \) and the sender’s public key \( y \).

We will let \( M', r', s' \) be the received versions of \( M, r, s \). To verify the signature the verifying program must check to see that \( 0 < r' < q \) and \( 0 < s' < q \) and if either fails the signature should be rejected. If both of the conditions are satisfied then we will compute

\[
w = (s')^{-1} \mod q
\]

\[
u_1 = ((SHA(M'))w) \mod q
\]

\[
u_2 = ((r')w) \mod q
\]

Then if \( v = r' \) then the signature is valid and if not then it can be assumed that the data may have been changed or the message was sent by an impostor.

**MATHEMATICAL MODEL**

In EAACK, Digital Signature is used to prevent the attackers from acknowledgment packets. All the parts of EAACK scheme (ACK, S-ACK, MRA) are acknowledgement based detection schemes. They all are relay on the ACK packets to detect malicious node in MANET network. Thus it is extremely vital to ensure that all acknowledgement packets in EAACK are authentic and contaminated. In another way, if the attackers are insolent enough to forge acknowledge packet all the three schemes will be vulnerable. To overcome this problem, we use Digital Signature Algorithm (DSA) [7] in IDS. To ensure the integrity of IDS, EAACK requires to all the ACK packets to be digitally signed before they are send out and verified when they are accepted by the receiver.

**Step 1:** A fixed length message is digested by using hash function \( H \) for every message \( m \), mathematically this can described as:

\[
H(m) = d
\]

**Step 2:** The sender Alice needs to apply its own private key \( Pr_{Alice} \) on the message digest \( d \) and produces result signature \( Sig_{Alice} \), which is attached to message \( m \) and Alice’s private key.

\[
Sig_{Alice}(d) = Sig_{Alice}
\]

The sender Alice is obliged to always keep her private key \( Pr_{Alice} \) as a secret without concealed to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice’s signature and send them to Bob. As these malicious message signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can attacks on the entire network and generate malicious attacks to Bob.

**Step3:** Alice can send message \( m \) along with the signature \( Sig_{Alice} \) to Bob via an unsecured channel. Bob then decrypts the received message \( m' \) against the pre agreed hash function \( H \) to get the message digest \( d' \). This process can be generalized as,

\[
H(m') = d'
\]

**Step4:** Bob can verify the signature by applying Alice’s public key \( Pr_{Alice} \) on \( Sig_{Alice} \) by using

\[
Sig_{Alice}(Sig_{Alice}) = d
\]
Step 5: If $d == d'$ then it is original message $m'$ transmitted through an unsecured channel is indeed sent from Alice and the message it itself is intact.

### H/W REQUIREMENTS

- **Processor**: Pentium iv 2.6 GHZ
- **Ram**: 512 MB DDR2 RAM
- **Monitor**: 15” color
- **Hard disk**: 20 GB
- **Floppy drive**: 1.44 MB
- **CD drive**: LG 52x
- **keyboard**: standard 102 keys
- **mouse**: 3 buttons

### S/W REQUIREMENTS

- **Front End**: Java and J2ME
- **Tools Used**: Eclipse
- **Operating System**: Windows XP/7

### OUTPUTS

#### 4. CONCLUSION

In this paper we have studied various IDS’s in MANET, with their merits and demerits. Our proposed IDS IEAACK scheme removes the weakness of watchdog approach (such as receiver collision, limited transmission power etc) and provides a secure end to end acknowledgement for all the nodes. Also we studied the digital signature algorithm is used to provide authentication of data and validating the sender. In the future, we plan to follow hybrid cryptography techniques to reduce the network overhead caused by digital signature.

### REFERENCES


