Implementation of EAACK Scheme in MANETs with Hybrid Cryptography Algorithm-ECC

Mattareddy S.
M.Tech (IT), Department of CSE, JNTUK, Kakinada, India
Email: syamalammattareddy357@gmail.com

Dr. Ch. Satyanarayana
Professor, Department of CSE, JNTUK, Kakinada, India
Email: chsatyanarayana@yahoo.com

Abstract -- Now a days we are moving towards wired to wireless networks from past few years. The quantifiability and quality brought by wireless networks create a potential in several emerging applications. Among the all the networks available in today market Mobile Adhoc NETworks (MANETs) is one in every of the foremost necessary and distinctive application. In MANETs mobile nodes are come in the range of mobility of nodes and they decide to co-operative for transferring data between the mobile nodes. For MANETs there is no predefined topology. Mobile nodes in MANETs are depend on neighbor nodes when transmission range beyond limit(i.e), multihop networks. Various security problems came because of MANETs properties. To avoid the security problems in MANETs we require an efficient intrusion detection system algorithm. In this paper we proposed a new IDS named EAACK with ECC algorithm to demonstrates more malicious misbehavior detection in networks and it is not greatly affect the network performances.

Keywords – MANETs, ECC, ACK, S-ACK, MRA, IDS, Digital Signature.

I. INTRODUCTION

MANET (Mobile Adhoc Network) refered as a multi-hop packet based wireless network self-possessed of a set of nodes that can commune and move at the similar time, with no using any kind of unchanging wired communications. MANET is in fact identity to classify and adaptive networks that can be twisted and collapsed on-the-fly without the need of any federal administration. If not, a stand for “Mobile Ad Hoc Network” A MANET is a type of ad-hoc network that can vary locations and organize their own on the fly. For the reason that MANETs are variable they use wireless associations to connect to a range of networks. This be able to be a normal Wireless-Fidelity connection, or a different intermediate, such as a cellular or dependency broadcast.

How MANET works?

The function of the MANET functioning group is to regiment IP routing protocol functionality appropriate for wireless routing request within both stationary and self-motivated topologies with enlarged dynamics due to node movement and other factors.

Approaches are proposed to be comparatively trivial in nature, appropriate for multiple hardware and wireless environments, and address scenarios where MANETs are deploy at the edges of an IP communications. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET terms and administration features.

With full-grown components from earlier work on investigational reactive and proactive protocols. MANET solves the problems 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.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes’ lack of physical protection, malicious attackers

![Fig.2. Structure of MANETs](image-url)
can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET’s distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. SYSTEM ANALYSIS

Existing System

By definition, Mobile Ad hoc NETwork (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. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes’ lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET’s distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

Disadvantages Of Existing System:

Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

Proposed System:

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK) with cryptographic algorithm ECC.

Advantages Of Proposed System:

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.

III. IMPLEMENTATION

Intrusion Detection Approaches:

ACK implementation

Secure Acknowledgment (S-ACK)

Misbehavior Report Authentication (MRA)

Digital Signature Validation & ECC

ACK implementation:

ACK is basically an end – to – end acknowledgment scheme. It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected.

The basic flow is if Node A sends a packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A), if ACK from the destination get delayed then it S-ACK process will be initialized.
Secure Acknowledgment (S-ACK):

In the S-ACK 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.

![S-ACK Scheme](image)

Misbehavior Report Authentication (MRA):

The MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

Digital Signature Validation:

In all the 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 ECC:

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.

IV. SYSTEM ARCHITECTURE

Number of discriminable detail in an image. There exits different Interpolation techniques which increase the resolution of an image. Interpolation increases the number of pixels in an image. Different Interpolation techniques are:
1. Nearest Neighbor Interpolation
2. Bilinear Interpolation
3. Bi-cubic Interpolation

In nearest neighbor interpolation, the new pixel is assigned with intensity of nearest neighbor in the original image. In bilinear interpolation, the interpolation is performed in one direction and then in the other direction. Here four nearest neighbors are considered for estimating the intensity of new pixel. Sixteen neighbors are considered for bi-cubic interpolation to estimate intensity of the new pixel [8].

The other techniques which increase the resolution are: Wavelet Zero Padding (WZP), assumes that the signal is zero outside the original support. The most common form of zero padding is to append a string of zero-valued samples to the end of some time domain sequence. Zero padding in the time domain is equivalent to optimal interpolation in the frequency domain, which restores the correct amplitudes. Single-frame resolution enhancement by Irani and Peleg, where four low-resolution images generated by rotation and translation from the input low-resolution image are used [1].

Now a days, Resolution Enhancement in Wavelet domain plays a major role in Satellite Image Processing [5], [7]. In which Continuous Wavelet Transform and Discrete Wavelet Transform (DWT) are the basic wavelet transforms. Out of which DWT is applied on satellite images to improve its resolution [6]. The discrete wavelets are classified into two categories i.e., Real Wavelets and Complex Wavelets. Because of the drawbacks of real wavelets like oscillations, shift variance, aliasing and lack of directionality complex wavelets are preferred over real wavelets [3]. The proposed technique is based on Complex Wavelet Transform (CWT) which is a complex valued extension to DWT.

If CWT is applied to a satellite image, it decomposes an input image into different sub-bands. That means it creates the transform coefficient sets. These coefficients are modified with a factor α/2 to produce the resolution enhanced image. The singular value decomposition (SVD) is used to enhance the brightness of the image by generating the new low frequency band.

V. EXISTING TECHNIQUE

The loss that is produced in interpolation techniques are high frequency components i.e., edges. The edge information is necessary for a good quality image. To preserve the edges of an image DWT technique is used. DWT decomposes the input image into set of four transform coefficients. They are LL, LH, HL and HH. The first letter corresponds to low pass or high pass filter applied to the rows and the second letter corresponds to low pass or high pass filter applied to the columns. These coefficients are modified to improve resolution. Stationary Wavelet Transform (SWT) is used in parallel to DWT to further improve the resolution of satellite image. The high frequency sub-bands are interpolated and are combined with sub-bands obtained from SWT. i.e., the high frequency sub-bands of DWT are modified by using high frequency sub-bands obtained through SWT. Inverse DWT (IDWT) is applied to generate reconstructed high resolution image [2].

The SVD is used to improve the brightness of the image in combination with DWT and Histogram Equalization. To get high contrast image, histogram technique is used.
The LL sub-band is estimated from the SVD of LL band and DWT applied to histogram equalized image. Then IDWT is applied to get an image with high resolution and brightness.

DWT considered here is a real wavelet. To overcome these drawbacks complex wavelets are preferred over real wavelets. The complex wavelets have good directional selectivity and Shift invariance. These features enables the complex wavelet transforms are preferable than other techniques. The proposed technique is based on CWT [1].

VI. PROPOSED TECHNIQUE

ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

PERFORMANCE EVALUATION

A. Methodology:
Enhanced adaptive acknowledgement (EAACK) is an acknowledgement based intrusion detection system; in order to ensure all acknowledgement packets is authentic. They use digital signature algorithm (DSA) to sign the acknowledgement packets, digital signature algorithm (DSA) involves more routing overhead and energy consumption. Adopting hybrid cryptography techniques. To further reduce the network overhead caused by digital Signature without compromising its security. Here we proposes ECC instead of DSA to ensure that all acknowledgment packets in EAACK are authentic and untainted. ECC stands for “Elliptic Curve Cryptography Algorithm”, it’s used to create a digital signature of data (a file for example) in order to allow you to verify its authenticity without compromising its security. [14]

ECC Algorithm:
While (True)
Do Read Data Packet;
Process it;
If (node is destination node) Then
Send Sack packet to previous node
Else
Start timer for PckID and wait for Sack packet to be received
If (Sack packet received in time)
If (PckID in Sack in list)
Remove PckID
And
its timer from list
Send Sack to previous node
Else
Send PckID Data Packet to all neighbours and
start timer and wait.
Receive acknowledgement from neighbour
If (SAck packet is from next node)
Remove PckID and its timer from list
Send Sack to previous node
Else
Report next node as malicious node
End While

B. Simulation Configurations:
In this paper we concentrate on describing the simulation environment and the system of methods followed in a particular discipline as well as comparing performances through simulation result comparison with EAACK schemes. Our simulation is conducted in machine which has java with version JDK 1.6 and above. We used NetBeans IDE 7.4 version with minimum 256 MB RAM the coding has been done to simulate the concept which has been discussed the ECC algorithm which is providing high security while packet are send through the network from node to node.

Encrypted message and Decrypted message is a function of key size and data size for both DSA and ECC. ECC key size is relatively smaller than DSA/RSA key size, thus encrypted message and Decrypted message in ECC is smaller as shown in below experimental results. These results provide high quality in data delivery with high Security provided by ECC.

VII. EXPERIMENT RESULTS

Node Creation

Node Information

Server node

ACK-SCHME

Detecting Malicious Nodes

Detecting Victim Nodes
S-ack scheme

Mra scheme

Applying algorithm

VIII. CONCLUSION AND FUTURE WORK

In this paper the main focus has been laid on comparative study of EAACK approach and its limitation with EAACK protocol using ECC. Here we have study the behaviour of EAACK technique. The algorithm is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report and to authenticate whether the destination node has received the reported missing packet through a different route and to achieve this we have to focus on the comparative study of ACK, SACK & MRA scheme. To extend the deserves of our analysis work, we plan to Investigate the subsequent problems in our future research:

1) Potentialities of adopting hybrid cryptography techniques to additional cut back the network overhead caused by digital signature;
2) examine the chances of adopting a key exchange mechanism to eliminate the necessity of redistributed keys;
3) Testing the performance of EAACK in real network environment rather than software code simulation.

REFERENCES


