International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, September 2015
www.ijates.com
ijates
ISSN 2348 - 7550

# IMPLEMENTATION OF EAACK SCHEME IN MANETS WITH HYBRID CRYPTOGRAPHY ALGORITHM-ECC

**Mattareddy S[1], Dr.Ch.Satyanarayana[2]**

*[1]M.Tech (IT), [2]Professor, Department of CSE, University Campus, Jntuk Kakinada Andhra Pradesh, (India)*

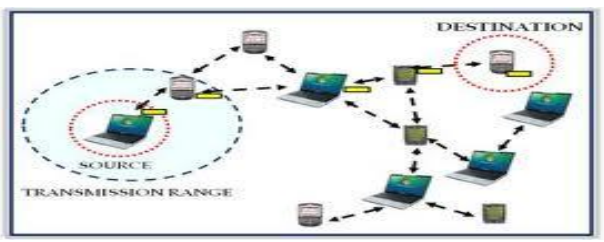
## ABSTRACT

*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 a efficient intrusion detection system algorithm .In this paper we proposed a new IDS named EAACK with ECC algorithm to demonstrates more malicious mis -behavior 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 Ad hoc 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.




**Structure of MANETs**

### 1.1 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 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

### 2.1 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. Existing scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog schemeis consisted of two parts, namely, Watchdog and Path rater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission.

### 2.2 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.

### 2.3 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.

### 2.4 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

### 3.1 Intrusion Detection Approaches

ACK implementation

Secure Acknowledgment (S-ACK)

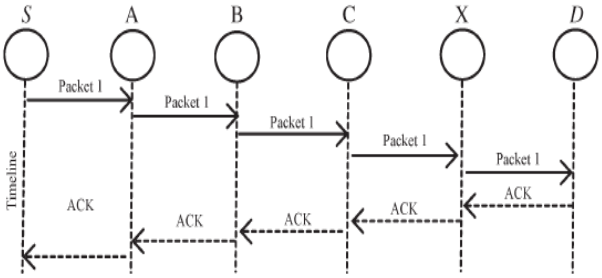
Misbehavior Report Authentication (MRA)

Digital Signature Validation & ECC

### 3.2 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.

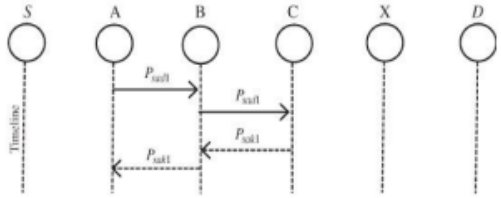
The basic flow is if Node A sends an packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A) , if ACK from the destination get delayed then it S-ACK process will be initialized.




**ACK Scheme**

### 3.3 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**

### 3.4 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.

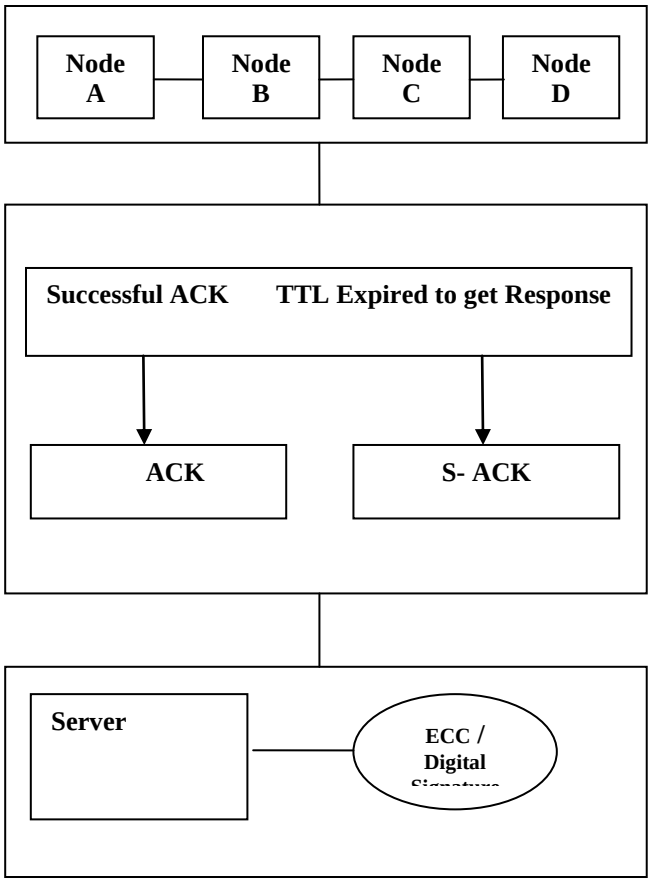
### 3.5 Digital Signature Validation

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.

### 3.6 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.

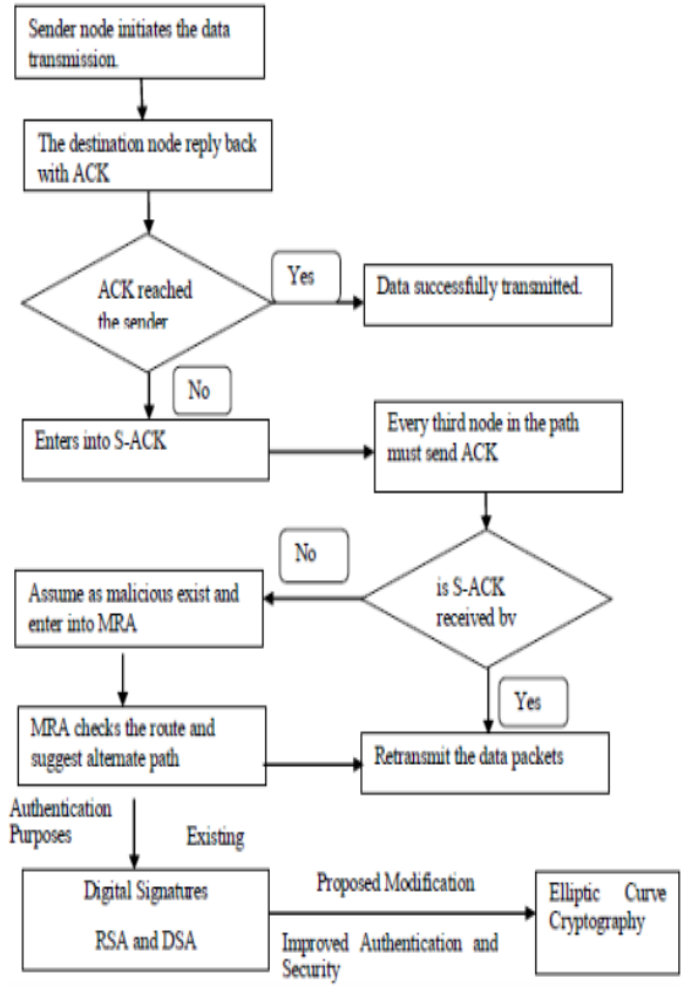
## IV.SYSTEM ARCHITECTURE




## V. 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.

Here it gives the step wise execution of the all the schemes in this project.first it cheks the ACK and then S-ACK,and then move to MRA scheme to find misbehavior nodes and then aplly the digital signatures for the scheme for providing security and authentication.




## VI.PERFORMANC EVALUATION

### 6.1 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]

### 6.2 Ecc Algorithm

While (True)

Do Read Data Packet;

Process it;

If (node is destination node) Then

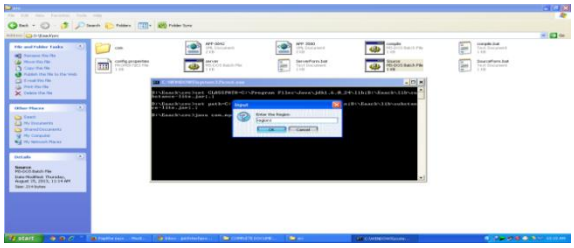
```
    Send SAck packet to previous node
Else
    Start timer for PckID and wait for Sack packet to be received
 If (SAck packet received in time)
     If (PckID in SAck in list)
          Remove PckID
     And
          its timer from list
          Send SAck to previous node
     End
Else
     Send 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
```

### 6.3 Simulation Configurations

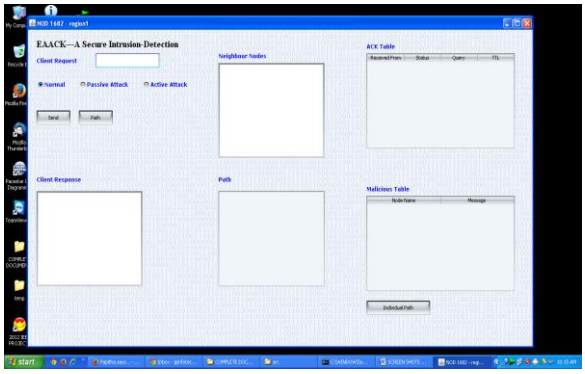
In this paper we concentrate on describing the simulation environment and the system of methods followed in a particular discipline as well as comparing performances through simulation result comparison with EAACK schemes. Our simulation is conducted in machine which has java with version JDK 1.6 and 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.

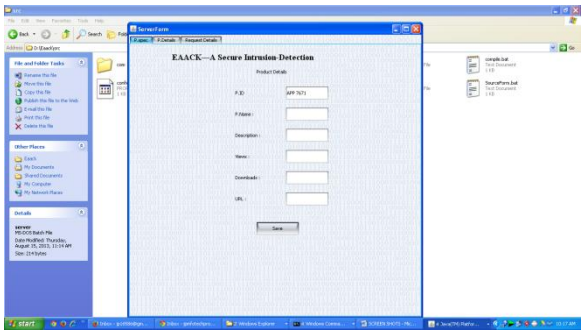
## VII. EXPERIMENT RESULTS



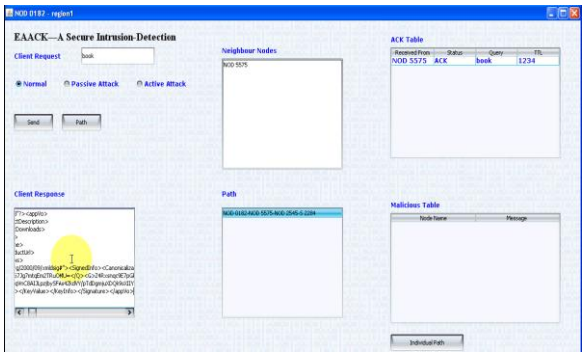
**Node Creation**




**Node Information**



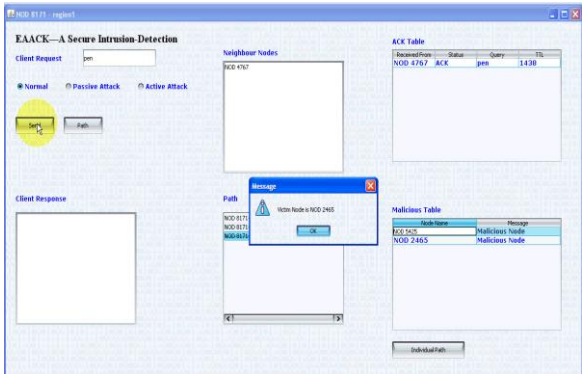

**Server Node**



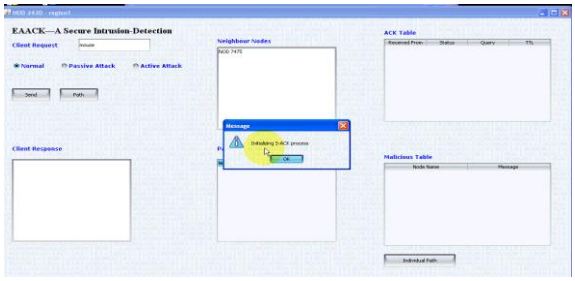

**Ack-Scheme**

ijates
ISSN 2348 - 7550

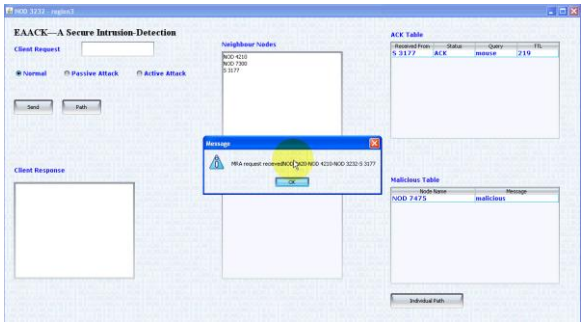

**Detecting Malicious Nodes**



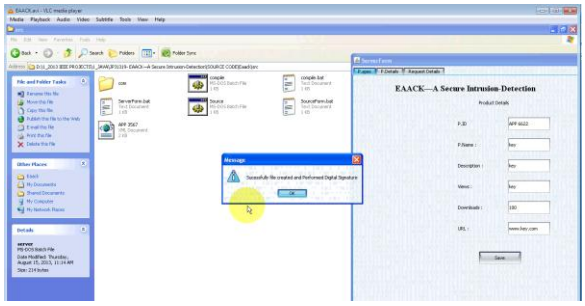

**Detecting Victim Nodes**



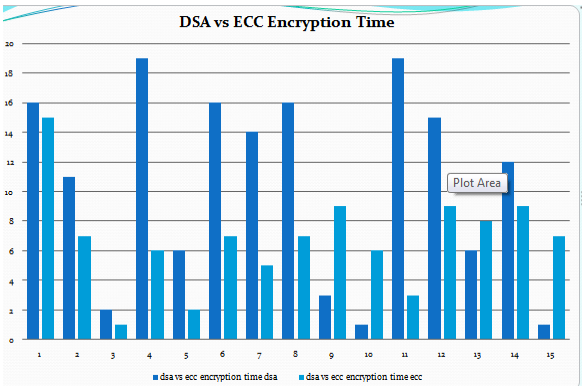

**S-Ack Scheme**



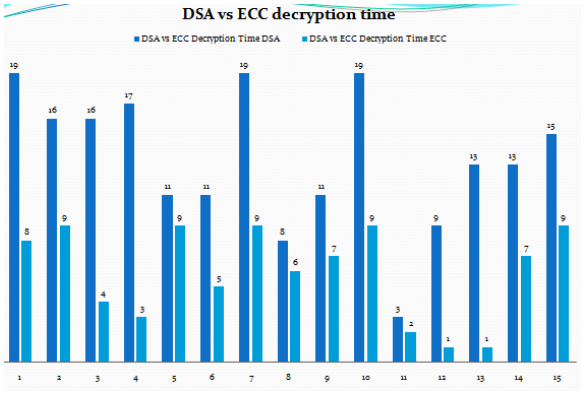

**Mra Scheme**




**Applying Algorithm**




**DSA Vs ECC Encryption time**




**DSA Vs ECC Decryption time**

## 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.And calculated the encryption and decryption times of the DSA and ECC algorithms.ECC is having the less key size so it will take the very less timefor Encryption compare to the DSA and same for the Decryption also. So , ECC performance well without disturbing the network activities.

. 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

[1]. Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on DEPEDABLE and Secure Computing, 2011.

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

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

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

[5]. D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[6]. 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.

[7]. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[8]. M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc ACM Workshop Wireless Secur., 2002, pp. 1–10.

[9]. Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[10]. 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 technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[11]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[12]. N. Kang, E. Shakshuki , and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[13]. V. Katiyar, K. Dutta, S. Gupta; "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment." International Journal of Computer Applications 11(10):41– 46, December 2010.

[14]. Xu Huang; Shah, P.G.; Sharma, D.; , "Protecting from Attacking the Man-in- Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange," Network and System Security (NSS), 2010 4th International Conference on , vol., no., pp.588- 593, 1-3 Sept. 2010.

[15]. Yong Wang; Ramamurthy, B.; Xukai Zou; , "The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks," Communications, 2006. ICC '06. IEEE International Conference on , vol.5, no., pp.2243-2248, June 2006.

**ABOUT AUTHORS**

| | |
|---|---|
|  | **MATTAREDDY S** received Diploma in Computer Engineering from Government Polytechnic, Hyderabad ,in 2009. Bachelor Degree in Electronics and Computer Engineering from KLCE , Guntur ,A.P., in 2012 and now pursuing M.Tech degree in Information Technology from University Campus , JNTUK, KAKINADA ,Andhra Pradesh . His research interests include network security , Data mining and MANETs. |
|  | **Dr.Ch.Satyanarayana** , currently working as a Professor in CSE Dept, UCEK, JNTUK, Kakinada. He has completed his Ph.D in Computer Science and Engineering. He worked as a Head of department, CSE, and worked as a controller of examinations for JNTU Kakinada. He has few decades of experience in teaching. He published hundreds of papers and attended many international conferences. |