ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Hybrid Cryptography for Secure Superior Malicious Behavior Detection and Prevention System for MANET's

Shreyas S. Jathe[1], Vidya Dhamdhere[2]

P.G. Student, Department of Computer Engineering, G.H.R.C.E.M, Savitribai Phule Pune University, Pune, India[1]

Asst. Professor, Department of Computer Engineering, G.H.R.C.E.M, Savitribai Phule Pune University, Pune, India[2]

ABSTRACT: Wireless network are used very rapidly and widely. Being mobile used in many fields. Mobile ad hoc network (MANET) is one of the most important applications of wireless networks. In which all the nodes work individually as a transmitter and a receiver. In this paper, we have proposed a system, which can provide high security when data is, send from one place to another place. The system is called as Hybrid Cryptography. Hybrid Cryptography gives a better security than the traditional approaches. In existing system less security provider is used. In this paper, to reduce network overhead, packet delivery ratio caused by existing system, we are using the concept of RSA and DES algorithm along with the digital signature. Compared to present approaches Hybrid Cryptography demonstrates higher malicious behaviour detection rates, in certain states while does not greatly affected the network performances.

KEYWORDS: MANET (Mobile ad hoc network), PDR (Packet Delivery Ratio), RSA (Rivest, Shamir, Adleman), DES (Data Encryption Standard).

I. INTRODUCTION

In now a day, wireless networks are much popular and easy to use rather than the wired network. Wireless network is using everywhere and in future because of more mobility and scalability. Wireless ad hoc network having a collection of "peer" mobile nodes, this "peer" mobile nodes are proficient of interacting and independently help each other without taking help of fixed infrastructure [1]. Nodes using routers for communication, which are out of range and similar range node, interact with each other via wireless links.

By definition, a mobile ad hoc network is a constantly self-configuring, self-maintained infrastructure less network of mobile devices, which are associated without wires [2]. Mobile ad hoc network consists of mobile nodes. These mobile nodes, which can communicate with each other in bidirectional way having wireless transmitting and receiving factor in network, directly or indirectly. We can communicate with each other by using wireless network and various components and maintained its mobility. If our nodes or components are not in the same range then we can use mobile ad hoc network. But to obtained this MANET which is divided into two different networks, called as single hop network, in single hop network, nodes which are present in the same range, they can interact with each other directly, i.e. no any common nodes used in between. But, in multi-hop network, we can use common nodes for communicating with each other to transfer and receiving the data, when there is a problem of communication with each other directly. Hybrid cryptography is consisted of major parts namely enhanced security services, attack prevention and misbehaviour report.

In this research work, the main purpose is to propose a new advanced system, which specially designed for MANET's, which solves not only security issues and services but also prevention and the false misbehaviour report problem to expand the research work to adopt a digital signature scheme during the packet transmission process. As in all acknowledgement base intrusion detection system, it is highly authenticated of all the acknowledgement packets.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

II. RELATED WORK

Elhandi M. Shakshuki, Nan Kang, Tarek R. Sheltami, author describe various intrusion detection in MANETs and its drawbacks. EAACK helps for solving false misbehaviour report problem and bring some new technique, which are identified with the enhanced adaptive acknowledgement. The methods, which are utilized, analyse the problem of ACK, TWO ACK and Watchdog scheme. The techniques depend on acknowledged packets; Digital Signature is used for preventing from attacker block from attacking the packets [6].

Nan Kang ElhadiM.Shakshuki and Tarek R. Sheltami, the author has represent the security which is depend on the acknowledgements packets, that how to shielded those packets from attacks and clarify intrusion detection system scheme for MANETs. Development which expands a minor in network overhead, utilizing EAACK2 which is called as enhanced adaption of EAACK, EAACK2 which implement better in the existence of false misbehaviour and partial dropping not just do a superior execution in the presence of forged acknowledgement packets, but also empower the packets purity when potential attack happen. The author additionally had an arrangement to inspect other confirmation plan and check outthe performance in the algorithm. Because of this, memory space of mobile nodes keeps better battery [7].

PanagiotisPapadimitratos, Zygmunt J. Haas, author gives description about the capability of the protocols to modify both malicious and benign faults grants fast and reliable data carrying in highly adverse network situation and examined various protocols like Secure Message Transmission (SMT), Secure Single Path (SSP), Transmission control protocol (TCP), Stream Control Transmission Protocol (SCTP) [11].

P. Joshi, P. Nande, A. Pawar, P. Shinde, R. Umbare explains about the MANETs are distributed is Intrusion Detection System. Explains about the features of EAACK that the system consist of a powerful attack control, which can help to guarantee the data security. Once the activator characterizes the keys to the nodes, automatically the preferences will be generated. And also explain that how they can detect as well as prevent from the malicious attacks [4].

B. Thanikaivel, B. Pranisa, author tells about the fast and secure data transmission in mobile ad hoc network using proactive and reactive system. In this paper, author uses the process algorithm and central agent for giving the security to the network. The disadvantage of proactive protocol is to wait for a new node when it is added to the network, it takes sometime to concentrate. For avoiding this drawback, reactive protocol is used. It increases the time efficiency and data transfer rate also increases [1].

III. PROBLEM STATEMENT

In this research work, a mobile ad hoc network involving intrusion detection system having three different types of nodes, a server node i.e. called as (source node), malicious node i.e. called as misbehaviour node and user node i.e. called as (destination node). We are implementing a system, which can be detecting the misbehaviour node in the network system when data, text or packets are transferred from source node to the destination node. The source node would do prevention of attack by not receiving the acknowledgement from the nodes, which are used in the system.

IV. OVERVIEW OF EXISTING SCHEMA IN INTRUSION DETECTION SYSTEM

Existing system is designed to overcome three of the six drawbacks of watchdog approach, as, false misbehaviour, limited transmission power and receiver collision.

Existing System with DSA Approach:

Existing system intrusion detection system contains DSA (Digital Signature Algorithm) which were used to sends the message with users access signature. Digital signature is an essential part of the cryptography.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Cryptography is branch of data security, which deals with study of encryption and decryption. It identical with parts of information security such as confidentiality, data integrity and authentication.

Digital signature schemes divides into two categories.

1) Digital signature with addition:

In the signature verification algorithm, it is requiring an original message. Example of consisting of a digital signature algorithm (DSA).

2) Digital signature with message reconstruction: This type of the signature itself in the confirmation process.

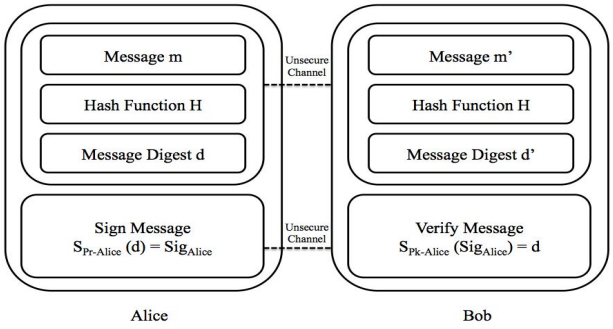

Figure 1. Working of DSA [6]

The general flow of information communication with digital signature is demonstrated in figure 1. In this, firstly the fixed length message digest is enumerated through a pre-agreed hash function *H* for each message *m.*

Second, the sender Alice must to apply its own private key on the digest message. Then Alice can send the message along with the digital signature through the unsecured channel.

Third, Bob has to computes the received message against the pre-agreed hash function for getting the digest message. After that process Bob needs to verify the signature by using Alice's public key.

V. PROPOSED SYSTEM

I. Hybrid Cryptography with RSA Approach:

A. *RSA Approach:*

RSA stands for the name of the three researchers who designed it, Ron Rivest, Adi Shamir and Leonard Adleman. Factorization of two major prime numbers is utilized as a part of RSA.

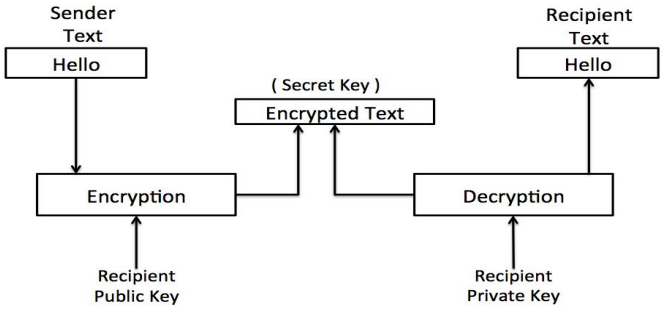

Figure 2. Working of RSA

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Public key are being utilized as a part of RSA for secure transmission of information or data. The required key for encrypting the data is public and for decrypting the data key is private which is shown in figure 2.

B. *RSA algorithm:*

1) Select two major prime numbers x and y.
2) For security guidance, the integers x and y which are chosen consistently at odd and should be of similar bit.
3) Compute m, such that the modules for both the private and public key i.e. m=xy.
4) Compute $\phi = (x-1)(y-1)$.
5) Randomly choose an odd integer t such that $t<\phi$ and such that t and ϕ comparatively prime.
$$(gcd(t,k)=1)$$
Where t is released as the public key exponent.
6) The formula of generating decryption key is $dk=t^{-1} \bmod \phi$
7) The pair by public key (t,k) and private key is dk.
RSA also named as "Public key Cryptography" which generally works with two keys i.e. public key as well as the private key. From the above algorithm, two keys are used and generated which is accessible to everyone is public key which is mutual key whereas not accessible to everyone is private key which is not a mutual key.

RSA also named as "Public key Cryptography" which generally works with two keys i.e. public key as well as the private key. From the above algorithm, two keys are used and generated which is accessible to everyone is public key which is mutual key whereas not accessible to everyone is private key which is not a mutual key.

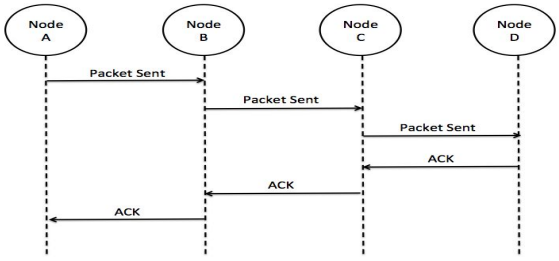

Figure 3. Previous system architecture

In previous intrusion detection system which is shown in figure 3, acknowledgement were sent to the previous nodes and from previous node to the server, this used to make intrusion detection system more complicated and time required for reaching the acknowledgement is getting increased. Time complexity of the given system is less than previous IDS [6].

C. *System Architecture:*

In figure 4, architecture is described as below

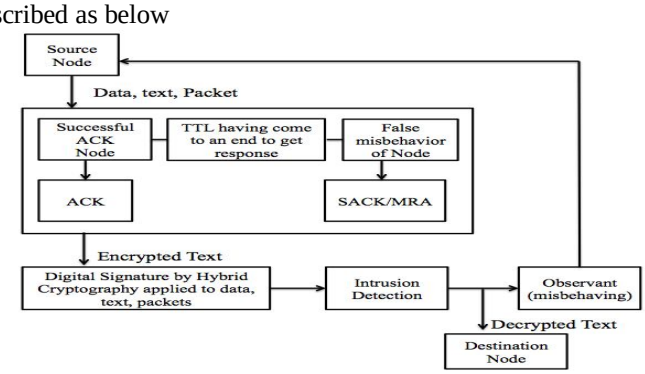

Figure 4. Proposed System Architecture [13]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Source node is used to send packets to the number of destination nodes therefore the activated path can be anyone. When packet is sent from the source node to the next node then back acknowledgement is sent to the source node, which is also called as activation node. When packet is sent from the next node then back acknowledgement is directly sent to the source node. When provided packet, text, data is reached at destination node then destination node sent back acknowledgement directly to the source node. At the same time, the text, data, packet is encrypted with digital signature at the source node. When data, text, packet is reached at destination node then packet, text, data, is decrypted at original message i.e., text, data, packet.

VI. NETWORK CONFIGURATION, ATTACK PREVENTION APPROACH

1. Network Configuration:

In network, new node addition in the network configuration. The network structure cycle goes through the three stages which are calling from the new node to the attacker or misbehaviour node then the concept of random key generation is used for the new node which are from activator i.e. (source node) and finally new network formation is done.

1) Sending request to the source node:
   Network formation is a type, system science that models how a system derive by ordering which factor change its design and how these system usually function.
2) Generating a random key:
   There are number of random key generation algorithms which can be utilized for keys for encryption. Random key is a particular altered function in java for generating a key.
3) At the point when a key is created for the new node, activator gets the request from the new node. In the activator database, activator stores all the information of another new node like IP address and machine address. At that point the activator will store every operation, which is settled on that node in the database.

2. Attack Prevention:

To build up the security in the mobile ad hoc network concept of Elliptic Curve Cryptography (ECC) is using for providing more security at the same time of sending packets from the source node to the destination node. ECC algorithm is basically utilized for the encryption and decryption of the data, text and packets [14]. While using the concept of encryption it creates secured connection, when data is to be send through the network and the observer cannot see the relevant information. The attack prevention system takes the precaution of providing prevention from the malicious node in the MANET. This system probably utilizing either RSA or DES for the concept of providing security data for the function of key exchange and encryption or decryption.

VII. PERFORMANCE EVOLUTION

Results:

In this section, study of impact of PDR (packet delivery ratio), RO or OFR (routing overhead or overflow rate), retransmission count and underflow rate are studied.

A. *Stimulation parameter:*

Parameter	Value
Number of Nodes	15 nodes
Simulation area	500 meter * 500 meter
Mobility Model	Dynamic Mobility
Speed range	Uniformly distributed (1-15) meter/second
Packet size	512bytes

Table 1.Simulation Parameter Table

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

B. *PDR (Packet Delivery Ratio):*
PDR is described as the ratio of number of packets received by receiver at destination node to the number of packets sends by the source node.

PDR= Total amount of data packet received (Receiver) / Total amount of packet sent (Source)

C. *RO or OFR (Routing Overhead or Overflow rate):*
This describes as the ratio of routing, which is related to the packets in bytes to the total routing and data transmission (sent or forwarded packets) in bytes.

RO = Σ (Routing Transmission) / (Σ(Data Transmission)+ Σ(Routing Transmission)).

D. *Performance Analysis:*

1. Result Scenario I:

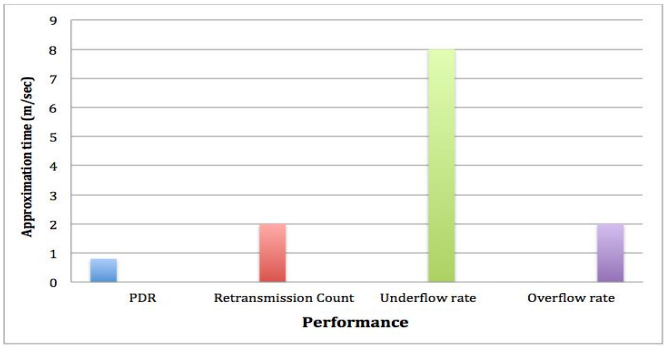

Figure 5. Result Performance I

In scenario I, we perform our system from 1 node to 3 nodes in which PDR, retransmission count, underflow rate and overflow rate is to be calculated which is shown in the figure 5.

2. Result Scenario II:

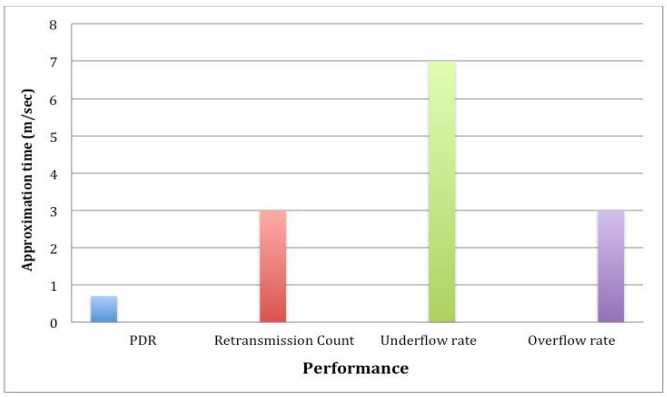

Figure 6. Result Performance II

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

In scenario II, we perform our system from 1 node to 7 nodes in which PDR, retransmission count, underflow rate and overflow rate is to be calculated which is shown in the figure 6.

3. Result Scenario III:

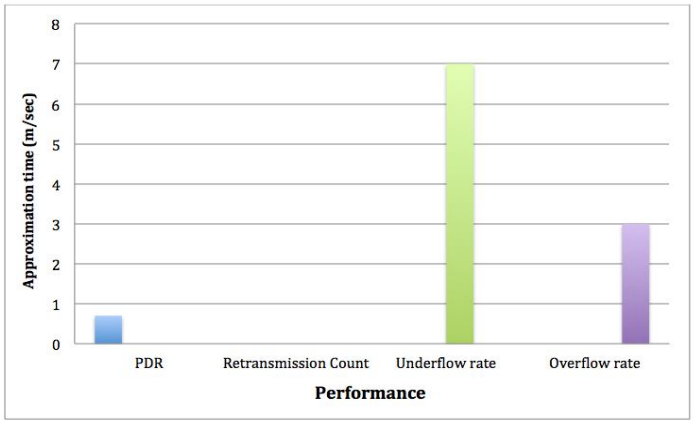

Figure 7. Result Performance III

In scenario III, we perform our system from 1 node to 11 nodes in which PDR, retransmission count, underflow rate and overflow rate is to be calculated which is shown in the figure 7.

4. Result Scenario IV:

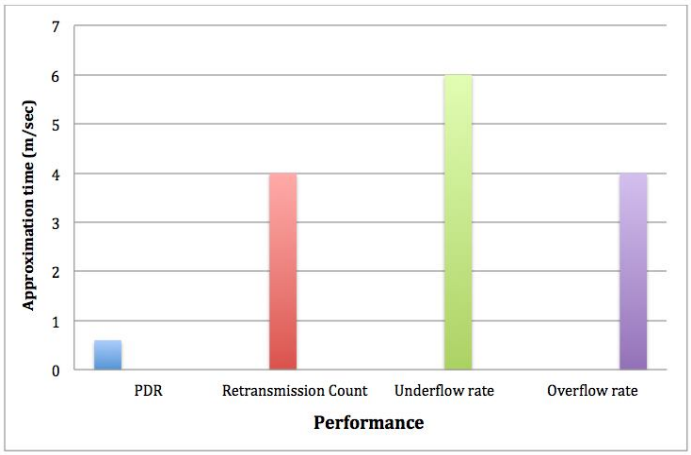

Figure 8. Result Performance IV

In scenario IV, we perform our system from 1 node to 15 nodes in which PDR, retransmission count, underflow rate and overflow rate is to be calculated which is shown in the figure 8.

VIII. CONCLUSION AND FUTURE WORK

The most discussed field when MANET's are concerned is Intrusion Detection System. Intrusion Detection System, which basically concentrate on preventing attacks, which are come from the attacker in the network, which can be harmful to the system. At the point when security issues are seen then packet dropping and hacking is the most

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

important concern in MANET's. For that we have given IDS named Hybrid Cryptography with some new techniques and methods for prevention of attacks, which are added.

There are some important features in the system:

1. This system has a powerful prevention control, which is one of the important and necessary conditions to guarantee the security of the data.
2. By providing Hybrid Cryptography technique, it will become difficult for attacker to break the network as well as retrieved the data.

We can extend our work in future that not using any kind of trusted third party (TTP) for key administration and could be recognized different attacks.

IX. ACKNOWLEDGEMENT

Apart from my own, the success of this paper depends largely on the encouragement and guidelines of many others. I am especially grateful to my guide Mrs.VidyaS.Dhamdhere, who has provided guidance, expertise and encouragement. Thanks to all those who helped me in completion of this work knowingly or unknowingly.

REFERENCES

[1] B. Thanikaivel and B. Pranisa, "Fast and secure data transmission in MANET," in *Computer Communication and Informatics (ICCCI), 2012 International Conference on*, Jan 2012.

[2] V. Gungor and G. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *Industrial Electronics, IEEE Transactions on*, vol. 56, no. 10, pp. 4258–4265, Oct 2009.

[3] B. D. Ramya K and S.H, "Hybrid cryptography algorithms for enhanced adaptive acknowledgement secure in manet," IOSR Journal of Computer Engineering (IOSR-JCE), Feb 2014.

[4] P. Joshi, P. Nande, A. Pawar, P. Shinde, and R. Umbare, "Eaack- a secure intrusion detection and prevention system for manets," in *Pervasive Computing (ICPC), 2015 International Conference on*, Jan 2015.

[5] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks",Wireless/Mobile Network SecurityY. Xiao, X. Shen, and D.Z. Du (Eds.) pp. 170 – 196, Springer2006.

[6] E. Shakshuki, N. Kang, and T. Sheltami, "Eaack- a secure intrusion- detection system for manets," *Industrial Electronics, IEEE Transactions on*, vol. 60, no. 3, pp. 1089–1098, March 2013.

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in manets," in *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, March 2011.

[8] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," *Mobile Computing, IEEE Transactions on*, vol. 6, no. 5, pp. 536–550, May 2007.

[9] A. R.L.Rivest and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," 1978.

[10] R. Jhaveri, S. Patel, and D. Jinwala, "Dos attacks in mobile ad hoc net- works: A survey," in *Advanced Computing Communication Technologies (ACCT), 2012 Second International Conference on*, Jan 2012.

[11] P. Papadimitratos and Z. Haas, "Secure data communication in mobile ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 343–356, Feb 2006.

[12] M. Athulya and V. Sheeba, "Security in mobile ad-hoc networks," in *Computing Communication Networking Technologies (ICCCNT), 2012 Third International Conference on*, July 2012.

[13] Shreyas S Jathe, V. Dhamdhere, "Hybrid cryptography for secure intrusion detection system for manets,"International Journal of Innovations & Advancement in Computer Science (IJIACS), 2014.

[14] P. M. Sanjith S and K. N, "Eaack based intrusion detection and prevention for manets using ecc approach," ,International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Aug 2013.

[15] RakeshShrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han* Department of Information & Communication Engg. Chosun University Gwangju, South Korea, " A Novel Cross Layer Intrusion Detection System in MANET",*24th IEEE International Conference on Advanced Information Networking and Applications, 2010.*

[16] Gang Xu, Member, IEEE, CristianBorceaMember, IEEE, and LiviuIftodeSenior Member, IEEE, "A Policy Enforcing Mechanism for Trusted Ad Hoc Networks",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 3, MAY/JUNE 2011.

[17] RaihanaFerdous, VallipuramMuthukkumarasamy, Abdul Sattar Institute for Integrated and Intelligent Systems Griffith University, Australia, "Trust Management Scheme for Mobile Ad-Hoc Networks" *2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).*