ADOPTING HYBRID CRYPTOGRAPHY TECHNIQUE FOR REDUCTION OF NETWORK OVERHEAD IN MANETs

Farzana Kauser[1]

[1]*M.Tech Student, Dept. of Computer Science and Engineering, Centre for Post Graduation Studies VIAT Muddenahalli, Chickaballapur District Karnataka India.*

Abstract

Mobile Ad Hoc Network is a infrastructure less network it is one of the most important and highly unusual application, which is famous among critical operations like warfare use, emergency recovery because of its self configuring nature of nodes. MANETs does not require any centralized administration, it dynamically forms a temporary network with the changing topology. Due to its open environment and irregular distribution of nodes MANET is vulnerable to malicious attack hence a new intrusion detection system named EAACK is introduced. This scheme demonstrates the complexity of malicious behavior detection rate in certain situations without greatly affecting the network performance. EAACK is a acknowledgment based intrusion detection system it is required to ensure that all the acknowledgment packets are authentic and unattained hence all the packets are signed digitally before they are sent out and till the receiver accepts, due to the usage of both digital signature and acknowledgment packet it causes a great network overhead. This paper proposes and enforces a hybrid cryptography technique in order to minimize the network overhead caused by digital signature.

Keywords: *EAACK, Hash algorithm, Wi_max 802.16, Caesar cipher, XOR cipher, XTEA.*

----------***----------

1. INTRODUCTION

The wireless network is preferred since its invention due to its natural mobility and scalability. MANET is a set of randomly moving nodes connected dynamically in arbitrary style which has the ability of both transmitter and receiver; the nodes communicate with each other through a wireless bidirectional link either directly or indirectly. The nodes cannot communicate between themselves when they are out of communication range hence MANETs is divided into two kinds that is single hop and Multi hop network. In a single hop network nodes communicate with each other directly when they are within same communication range whereas in multi hop the nodes depend on intermediary nodes when the nodes are out of the communication range. Less configurations and quick installation make MANETs to use in emergency situations. MANET is popular among critical mission applications there by network security is of much important. The open environment and irregular distribution of nodes in MANET make it possible to various types of attacks. MANETs are infrastructure less network they does not require any centralized administration they dynamically forms temporary network with changing topology. Mostly, in MANET routing protocols presume that each and every node in the network behaves conjunctively with other nodes presumably not malicious; attackers can easily compromise nodes by inserting malicious or non cooperative nodes in the MANET. The access points are like base station nodes which keeps record of connection, disconnection and flow of traffic in the network .It is difficult to find the membership of MANET environment as the nodes moving freely can join and leave network independently as they wish hence there is no guarantee that the path between the nodes is free from malicious nodes which may attempt to harm the entire network, a small number of adversary nodes may collapse the entire network Under such circumstances it is required to develop an intrusion detection system there are many intrusion detection systems proposed watchdog is popular among them. EAACK is a new intrusion detection system which is specially designed for MANETs to resolve three of six weakness of watchdog and to detect malicious behavior in the network. Digital signature is to protect the packets from being forged by the attackers, when there is more number of malicious nodes in the network there will be more acknowledgments and the usage of digital signature will obviously more this causes great network overhead which can reduced by adopting a hybrid cryptography technique. In further section we concentrate on the background information to better understand my research topic.

2. BACKGROUND

Enhanced Adaptive Acknowledgment (EAACK) is a new intrusion detection system[1] it is based on the previous work of [4] in this scheme digital signature is introduced to prevent the packets from being forged by the attackers. Enhanced Adaptive Acknowledgment (EAACK) which solves three out of six weakness of watchdog this technique depend on acknowledgment of packets so it include digital signature to prevent the attackers attacking packets.

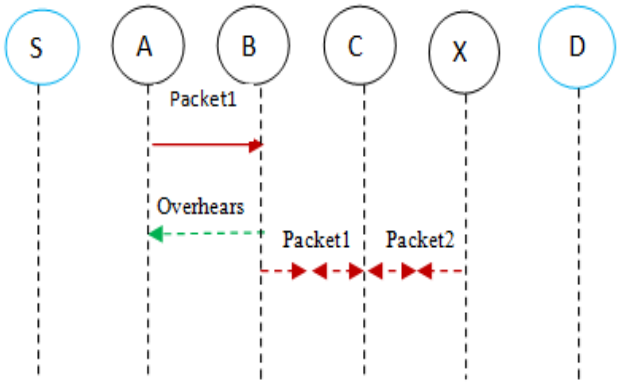

Fig-1: Receiver collision occurs at node c because both nodes B and X send packets at same time.

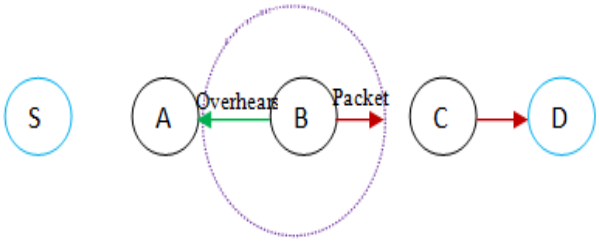

Fig-2: Limited transmission power problems lead C unable to receive packet1 from node B but it can be overheard by node A

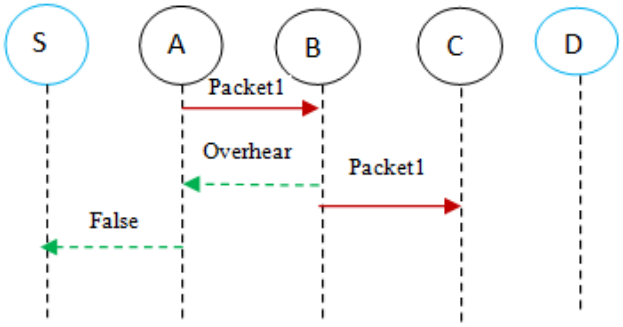

Fig-3: False misbehavior report sent by node A to source node S that node B is malicious even though node B forwards packet1 to node C.

EAACK consists of three parts namely:

1. Acknowledgment
2. Secure acknowledgment (S_ACK)
3. Misbehavior report authentication (MRA)

1) Acknowledgment: it is an end to end acknowledgment scheme which aims to reduce the network overhead when no adversary nodes in network are detected. Fig-4 describes the working of acknowledgment scheme, source node s first sends packet pckt1 to destination node D if there is no adversary node between source and destination the intermediary nodes simply forwards the packet pckt1 to destination and finally the destination need to send back an acknowledgment packet pack1 to source S within some specified time otherwise it switches to the secure acknowledgment mode.

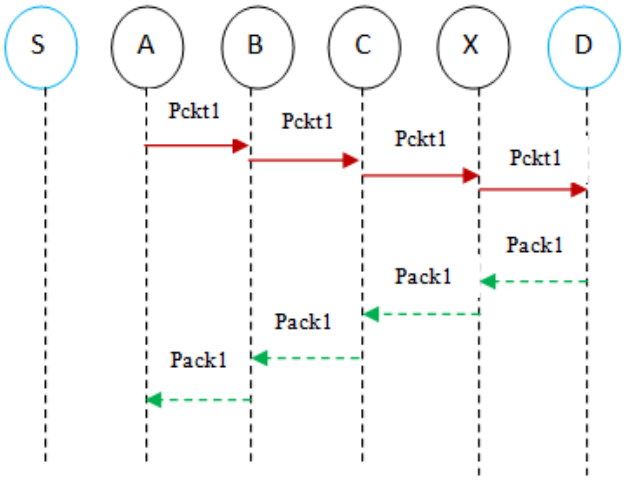

Fig-4: Acknowledgment scheme

2) Secure Acknowledgment (S-ACK): is proposed by Liu et al[2] it is improved version of TWOACK, the procedure is to let every three consecutive nodes to communicate with one another, finally the third node need to send back a secure acknowledgment packet to first node in reverse order of the same path within certain specified time otherwise the two nodes that is second node and third node is reported as malicious nodes and node1 generates a misbehavior report and sends to source node S.

3) Misbehavior report authentication (MRA): is designed to resolve the problem of watchdog that is it fail to detect adversary nodes in the presence of misbehavior report. To initiate MRA mode the source first searches its local knowledge domain and finds the alternate route to the destination if there is no other route except the existing route it starts DSR routing request to find another route to destination. To find misbehavior report node the destination node searches MRA packet in its local knowledge domain and compares whether the packet is already received via other route, if received then it concludes that it is a false misbehavior report and the node who generated this report it will be marked as malicious node, otherwise it trusts misbehavior report and accepts.

4) Digital signature: since Enhanced Adaptive Acknowledgement is an acknowledgment based intrusion detection system it is required to ensure that all the acknowledgment packets are authentic and unattained. In order to obtain the integrity of intrusion detection system, EAACK requires all packets to be signed digitally before sending out and until receiving, the network performance is affected due to the usage of both acknowledgment packet and digital signature which causes great network overhead.

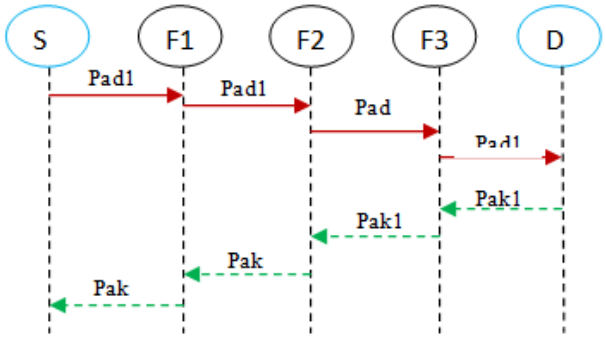

Fig-5: Enhanced Adaptive Acknowledgment

3. DESIGN AND IMPLEMENTATION

This paper, proposes a hybrid cryptography technique to minimize the network overhead; The overhead increases as the count of malicious nodes in the network increases. Here we have used hybrid routing protocol that is AODV and DSDV these are reactive and proactive protocols respectively, it is responsible for finding route between source and destination and reducing network overhead. Cryptography is a mathematical technique used for encryption and decryption of data, in this we proposed hash algorithm to ensure data integrity and the RC5 algorithm is designed to achieve high security when suitable parameter values are chosen it has three modules i.e. two's complement, XOR and Rotation , it requires less memory

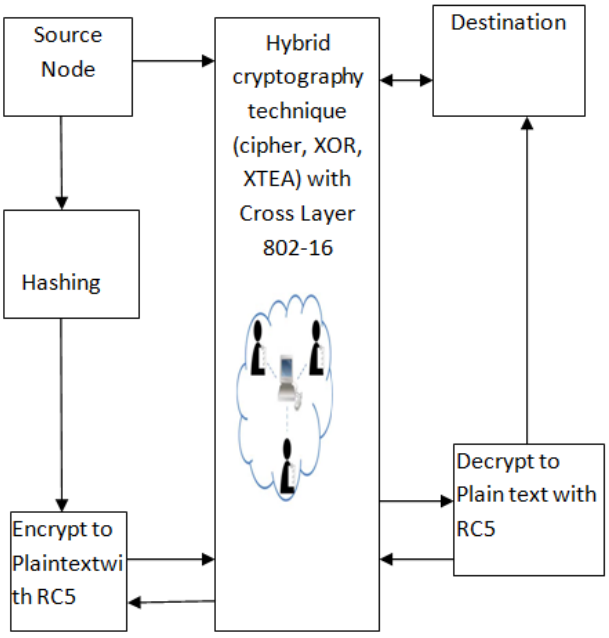

Fig-6 : System Architecture

compared to other cryptography algorithms.after encryption packet is sent through Wi-max. Wi_max standard IEEE 802.16 is similar to Wi-Fi which aims to deliver connection to network it uses Qos based on connection between base station and nodes and few more cryptographic algorithms such as CAESAR cipher, XOR cipher and XTEA, are used as hybrid cryptographic technique which reduces network overhead.

Table.1 parameter values for MANET simulation

MAC Protocol	802.16
Routing protocol	AODV, DSDV
Agent Type	Security
Terrain Size	1000x1000
Number of nodes	40
Node placement	Random
Number of sources	Node 0
Number of Sink nodes	Node 20

In cryptograph to correct the weekness of TEA, XTEA algorithm is designed XTEA is a incomplete unbalanced fiestel network block cipher it works on variable length block it does not require any initialization XTEA encrypts 8bytes value and 16 bytes key. In XTEA the plaintext splits into two halves in each round the right side is first shifted left four and right five these two values are xored with each other the result is added with original right side . The length of plaintext is equal to length of XTEA, XTEA is more secure than CAESAR cipher and XOR cipher.

4. SIMULATION CONFIGURATION

Our simulation work is held within the network simulator NS 2.31 on the platform windows XP operating system which creates a Unix environment this is performed by a tool called cygwin. The simulation is running on a laptop with core T4300 CPU and 2GB RAM. The NS2.31 configuration contains '40' nodes in a flat space of 1000X1000m with one source and destination with possible routes. Both physical layer and Wi_max 802.16 are included in the wireless elongation of NS2. The dynamic speed of mobile nodes has been limited to 10ms. UDP traffic with CBR is designed with a packet size of 512 bytes. The data packets are routed using AODV, DSDV routing protocols. The MANETs security performance depend on cryptography algorithms we have used four cryptography algorithms that is Rc5 CAESAR cipher, XOR cipher and XTEA algorithms. The NAM animator provides nodes, links, queues , packets and agents.

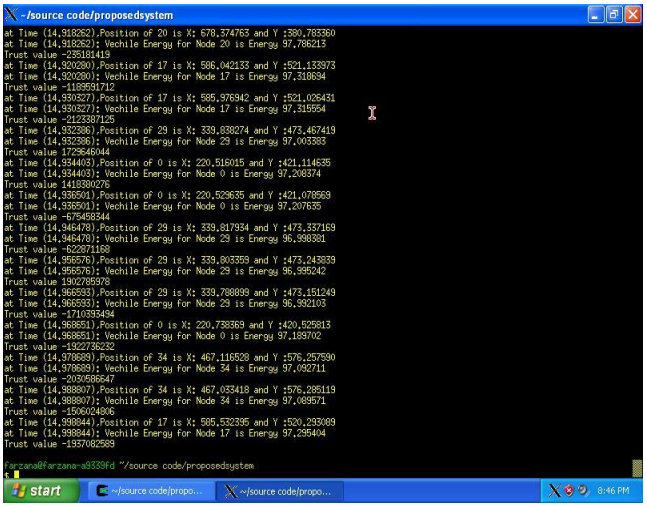

Fig-7: trust value.

To find whether the route is trusted or attacked by malicious node we calculate trust value by location of each node in the topology if the value is negative then the route is attacked by malicious node else the route is trusted.

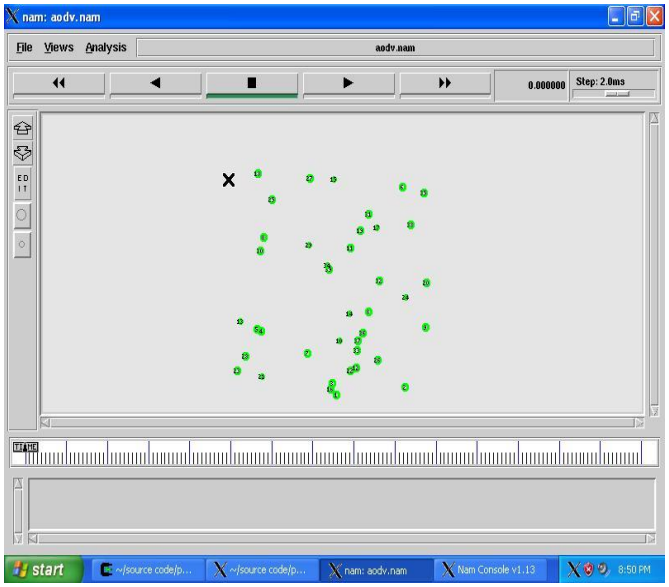

Fig- 8 : MANET environment

The simulation configuration contains 40 nodes which are distributed in arbitrary style there is still no connection between nodes only MANET environment is created as shown in fig-8.

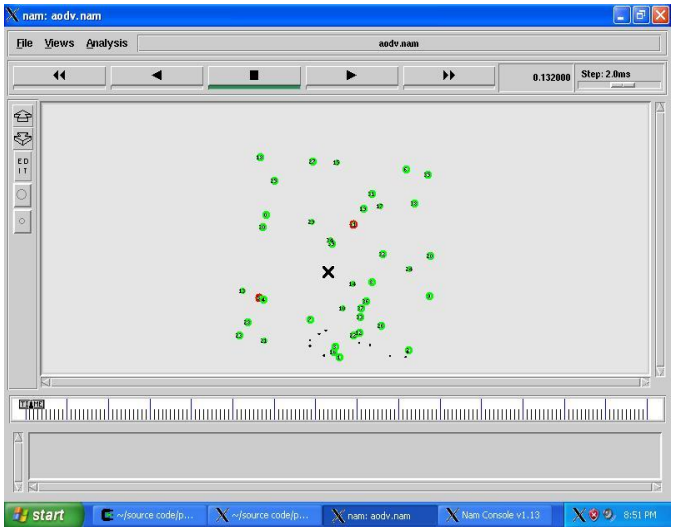

Fig-9 Detecting intruder

In the MANET environment malicious nodes are detected which drops all the packets and gives false report during packet transmission. Malicious nodes are detected by sending S-ACK and false report is detected by activating MRA mode. In the fig-9 the red circled nodes are malicious nodes which performs malicious activity in the network.

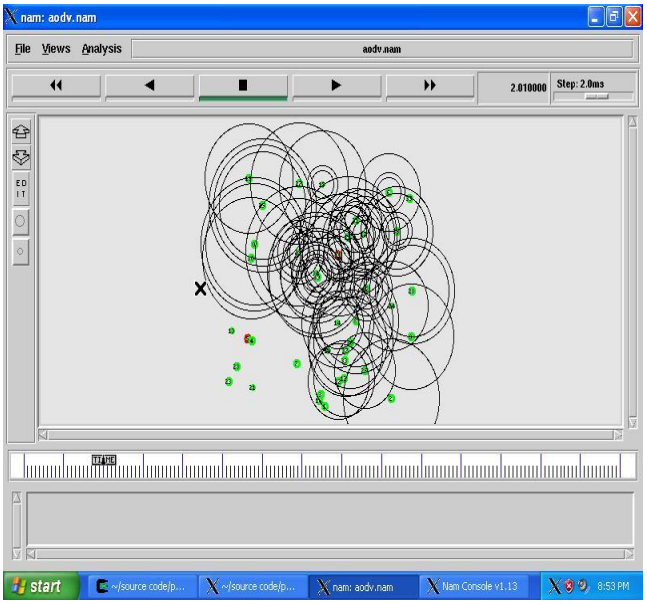

Fig- 10: NAM output shows signal propagation of nodes in MANETS

In the fig-10 in the MANET environment node 0 is source node sends packets to node 20 the nodes which are in red color are malicious nodes due to malicious nodes in the route node 0 changes route and sends packet, here the propagation takes place while data transmission.

5. PERFORMANCE EVALUATION

In order to measure performance of our proposed model we have three metrics i.e. routing overhead (RO), Packet delivery ratio (PDR), and end to end delay.

1. Routing overhead (RO) : is the ratio of routing related packets to the total routing and data transmission packets

$$RO = \frac{\sum Routing\ transmission}{\sum Data\ transmission + \sum Routing\ transmission}$$

The routing overhead is reduced by the usage of cryptographic algorithms i.e. CEASAR cipher, XOR cipher , XTEA algorithms and hybrid protocol.

2. Packet delivary ratio (PDR) : The ratio of total number of packets received by destination to the total number of packets sent by source.

$$PDF = \frac{\sum Received\ packets\ by\ destination}{\sum sent\ packets\ by\ source}$$

3. End to end delay : is for all successfully received packets, it is calculated for each packet by substracting the sending time from the destination time.

$$D = \frac{\sum_{1}^{N}[Treceived - Tsent]}{N}$$

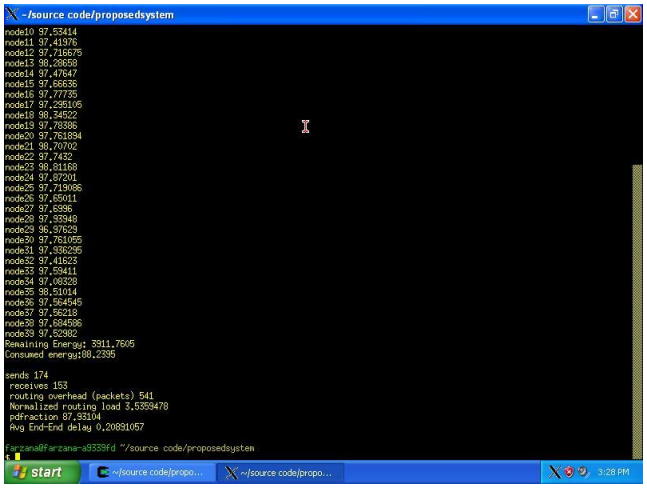

Fig- 11 : Full Simulation result.

Fig- 12 : Network overhead

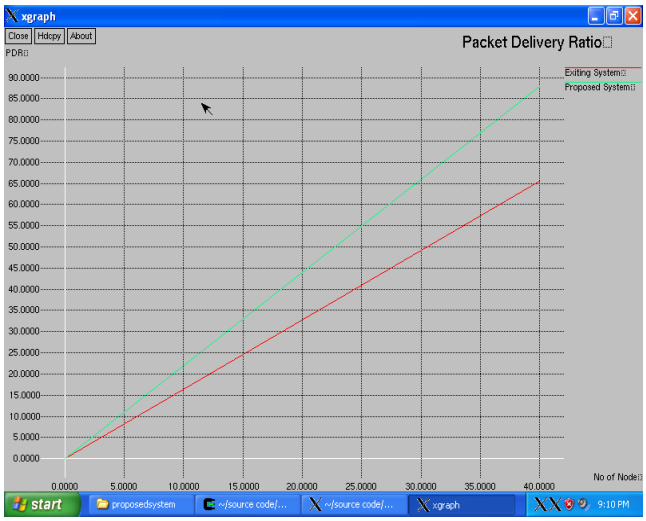

Fig-13: Packet delivery ratio

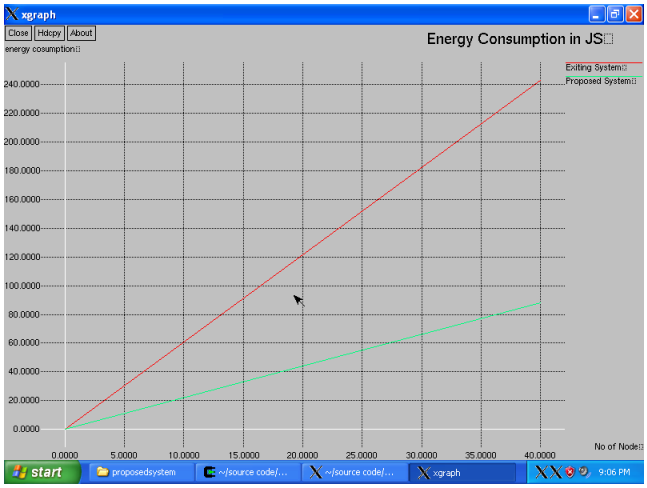

Fig-14: Energy consumption

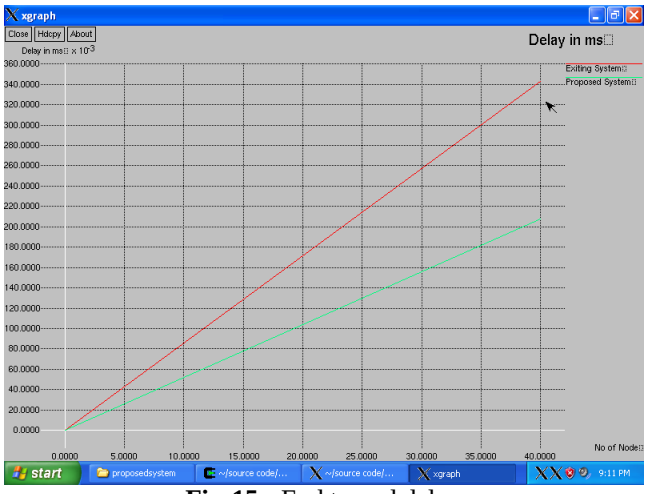

Fig-15 : End to end delay

6. CONCLUSION

The major drawback in MANETs security is Packet dropping attack hence a new IDS EAACK is proposed which provides security to the nodes by using digital signature and resolves few issues of watchdog IDS. EAACK performs better comparing to the basic techniques. Due to the usage of digital signature and acknowledgment packets, burden in the network increases which causes great network overhead this can be reduced by hybrid cryptographic technique, it uses hash algorithm and rc5 for security and Wi_max 802.16 is used as cross network layer which provides connection in network thereby packet loss will be less and the network overhead is reduced to some extent.

FUTURE WORK

Examine the possibilities of acquiring a key exchange process to remove the necessity of pre-distributed keys

REFERNCES

[1]. S. Marti, M. Baker, T.J. Giuli, and K Lai , “Mitigating routing misbehavior in mobile ad hoc networks”,in proceeding 6th Annual. International. Conference on Mobile Computing, Networks Boston, MA, 2000, pp. 255-265.

[2]. K Liu, P.K Varshney , J.Deng, and K.Balakrishnan , "An acknowledgment –based approach for the detection of routing misbehavior in MANETs" ,IEEE Transaction on Mobile Computing., volume. 6, no.5,pp.536-550, May 2007.
[3]. Sheltami, N.Kang and E.Shakshuki, "Detecting forged acknowledgements in MANETs, on proceeding. IEEE 25th International Conference .AINA, Biopolis, Singapore, March 2011.pp488-494.
[4]. Nan Kang, Tarek R .Sheltami, IEEE Elhadi M. shakshuki, senior member, IEEE, EAACK- A Secure Intrusion Detection System for MANETs, IEEE Transaction on Industrial Electronics, vol.60, No.3, March 2013.
[5]. A technique for obtaining digital signature and public key cryptosystems -R. Rivest, A. Shamir, L. Adleman, Communication .ACM, volume .21,No.2,pp.120-126,Feb 1983.
[6]. William Stallings, "Cryptography and Network Security", Fourth Edition, June 3, 2010.
[7]. G.Gopinath, G.Jayakumar MANETs routing protocol-A review volume .3, No.8, pp 574-582, 2007.
[8]. J.Wu and T.Anantvalee, A Survey on trespass Detection in Mobile Ad hoc Networks, New York Springer 2008.
[9]. Minimized Routing Protocol in Ad-hoc Network with Quality Maintenance Based on Genetic Algorithm: A Survey, Manisha, Upasna, jyoti chauhan, IJSRP, Volume .3,Issue 1,January 2013.
[10]. S.Patel, R.H Akbani and D.C.Jinwala, DOS attacks in MANETs, A Survey in Proeedings. 2nd int. Meeting ACCT ,Rohtak, Haryana, India, 2012,pp.535-541.
[11]. A Secure data transmission in MANETs using hybrid scheme, Syam gopi, Sowmya Thomas , IJERT, Volume 2, Issue 8, August 2013.
[12]. Hybrid cryptography by the implementation of RSA and AES algorithms , palaniswamy, V. Jeneba Mary, International journal of current research vol.33, Issue 4, pp. 241-244, april 2011 .
[13]. Sheltami, N Kang, and E Shakshuki , Detecting malicious nodes in MANETs, in Procedings. 12th International Conference. IIWAS, November 2010,pp.216-222.
[14]. N.Nasser and Y.Chen, Enhanced trespass Detection Systems for discovering malicious nodes in mobile ad hoc networks, in procedings. IEEE International conference on communication, Glasgow, Scotland, June 2007, pp.1154-1159.

BIOGRAPHY

Farzana kauser, completed B.E in information science and engineering from Dr.SMCE Bangalore now currently pursuing M.tech in computerscience and engineering from vtu centre for post graduate studies VIAT, chickaballapur district.