Implementation of HMAC-SHA256 Algorithm for Hybrid Routing Protocols in MANETs

Dilli Ravilla [*1]
[*1]Sr. Asst. Professor, Dept. of ECE, MIT, Manipal University,
Manipal, India dilli.ravilla@gmail.com

Dr Chandra Shekar Reddy Putta[*2]
[*2] Professor Coordinator, Dept. of ECE,
JNT University, Hyderabad, A.P, India.drpcsreddy@gmail.com

Abstract: **The purpose of a hash function is to produce a "fingerprint" of a message or data for authentication. The strength of the Hash code against brute-force attacks depends on the length of the hash code produced by the algorithm. Constructing the Message Authentication Codes (MAC) from Cryptographic hash functions (SHA-256) gives faster execution in software than symmetric block ciphers like Data Encryption Standard (DES) and also the library code for cryptographic hash functions are widely available. Here we implemented the HMAC-SHA 256 Algorithm for the message authentication and Data Integrity. This algorithm is introduced in hybrid routing protocol for Mobile network environment and the performance of the protocol is analyzed by calculating throughput, packet delivery ration and end-to-end delays of the network. The simulation is carried out using Network Simulator 2 (NS2). We observed that there is an improvement in throughput and packet delivery ratio at the cost of more processing time.**

Keywords: Message Authentication Code (MAC), Data Encryption Standard (DES), Cryptographic Hash function, Data Integrity, Network Simulator, Packet Delivery ratio.

I INTRODUCTION

The goal of security in MANETs is to provide security services to defend against all the kinds of threat. Attacks on *ad hoc* wireless networks can be divided into two types, namely, passive and active. A passive attack does not disrupt the operation of the network; it occurs when an attacker tries to eavesdrop on the data or the network traffic without altering it. This can violate the requirement of confidentiality if an adversary is also able to interpret the data gathered through snooping. This type of attack is less harmful than an active one, but is much harder to detect, because the attacker does not interfere with the operation. One way of overcoming such problems is to use powerful encryption mechanisms to encrypt data being transmitted, thus making it impossible for eavesdroppers to obtain any useful information from the data overheard. An active attack, by contrast, is one where the attacker actively seeks to modify, abstract, alter or destroy the data being exchanged, thus disrupting the normal functioning of the network. Any protocol which provides security in an ad hoc network should have the following features: confidentiality, integrity, availability, authenticity and non-repudiation [7, 8].

Confidentiality It refers to the protection of information from disclosure to unauthorized parties. Information about location in war fields, bank account statements, trade secrets are few examples where the confidentiality is necessary. Access to these information by unauthorized persons leads to destructive consequences.

Integrity guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.

Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

Non-repudiation ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

Message authentication is a mechanism used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid. Symmetric encryption provides authentication among those who share the secret key. Encryption of a message by a sender's private key also provides a form of authentication. The two most common cryptographic techniques for message authentication are a message authentication code (MAC) and a Secure Hash Function. A MAC is an algorithm that requires the use of a secret key. A MAC takes a variable length message and a secret key as input and produces an authentication code. A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message. A hash function maps a variable-length message into a fixed length hash value, or message digest. For message authentication, a secure hash function must be combined in some fashion with a secret key.

II Security In Hibrid Routing Protocol

In this paper, we implemented two secure routing techniques: HMAC-SHA256, a keyed-Hash Message Authentication Code – Secure Hashing Algorithm 256 is used for Authentication and Data Integrity which uses a secret key along with the hash function to send data from source to destination in a secure way and a Trust-Based system that prevents the Denial-of-Services (DoS) Attacks in the Network Simulator 2 (NS2) simulation environments in Ubuntu 13.10, Linux Operating System (OS). Scenarios are created with malicious nodes and implement attacks in the simulation environments and measure the performance parameters of the network with different zone pause time and increasing the number of mobile nodes along with the malicious nodes.

A. HMAC Algorithm

Digital signature is used to achieve message integrity, authentication and non-repudiation. In this process the sender uses a signing algorithm and its private key to sign the message. The message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm on the message-signature pair. The verification algorithm requires a verification key, which is a public key provided by the signer, to verify the document. After verification if the result is true, the message is accepted; otherwise, it is rejected. Hashing can be used for the digital signature process where the message is passed through an algorithm called cryptographic hash function or one-way hash function before signing. It is an algorithm which creates a compressed image of the message in the form of a hash value (or message digest) which is usually much smaller than the message and unique to it. Any change to the message will produce a different hash result even when the same hash function is used.

The HMAC-SHA256 [9] can be expressed as follows:

$$HMAC\ (K, M) = H((K \oplus opad) \parallel H((K \oplus ipad) \parallel M))$$

Where, H is an embedded hash function (in our case SHA256). K is a secret key padded to the right with extra zeros to the input block size of the hash function, or the hash of the original key if it's longer than that block size. M is the message input to HMAC. $\parallel$denotes concatenation.. $\oplus$ denotes XOR operation.
opad = 01011100 (0x5c)repeated b/8 times
ipad =00110110 (0x36) repeated b/8 times

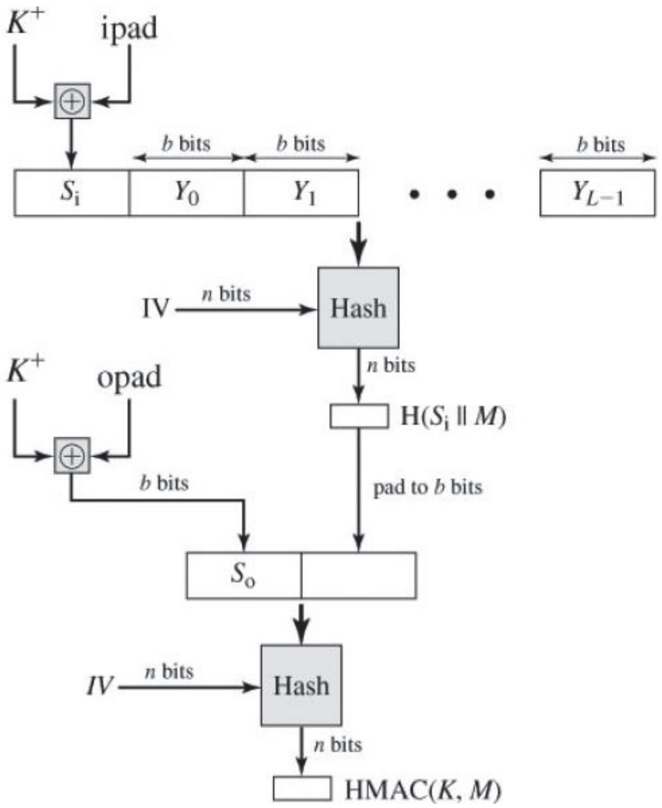

Figure 1: HMAC Structure

In words, step 1: Append zeros to the left end of K to create a b-bit string K+. 2. XOR K+ with *ipad* to produce the b-bit block S_i. 3. Append M to S_i. 4. Apply H to the stream generated in step 3. 5. XOR K+ with opad to produce the b-bit block S_0. 6. Append the hash result from step 4 to S_0. 7. Apply H to the stream generated in step 6 and output the result.

III HMAC-SHA256 Implementation

The SHA256 is used for authentication [10] and hashing in the HMAC procedure. In this section, we analyze the results of the SZRP implementation in NS2 simulation environment.

In this section the output of the HMAC-SHA256 algorithm as discussed in previous section is analyzed in the CodeBlocks IDE in the Ubuntu 13.10 OS.

Here for the illustration, the data is taken to be:
Data: Manipal Institute of Technology
Secret Key: Security
Result:
HMAC-SHA256 = 9299F475 081153C0 0D8C88D0 9C934664 1691C091 BDAC0359 B89619CA 8FD48736

A. ZRP Analysis (with HMAC-SHA256)

For the implementation point of view we use the ZRP patch in ns-2.33-allinone package. It is a version of NS2. We further analyze the performance of the secure ZRP with HMAC-SHA256 implementation and compare it at different zone radius keeping the number of nodes to be constant. The modifications that we made to the existing ZRP to model SZRP are:

i. The additional fields are introduced to perform security mechanisms like the Public Key, the Digest, the unique identifier, and the Signature. However, all the packets need not to contain these fields.

ii. The neighbor table of each node is increased by two fields; First field is to store the Public Key of its neighbors in each entry, while the second one is to indicate the trust level factor of that neighbor.

iii. Alarm Packet is used to declare malicious nodes when the trust value becomes zero.

B. Performance Metrics

Packet Delivery Fraction (PDF): This is the ratio of the data packets generated by the CBR sources to those delivered to the destination.

Routing Overhead (packets): This is the ratio of control packet overhead to data packet overhead over all hops.

End-to-End Delay: This is the average delay between the sending of data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays due to route acquisition, buffering and processing at intermediate nodes.

TABLE I
Simulation Parameters For SZRP

HELLO Message Interval	1.0 s
Allow HELLO Loss Packets	3 packets
Link State Message Interval	3.0 s
Zone Radius	Variable
Hash Length	160 bits
Signature Length	160 bits
Public Key Length	160 bits

In comparison to conventional ZRP, the SZRP has a higher delay because of the extra time taken for the HMAC-SHA256 processing. Figure 2 gives a clear comparison of ZRP and SZRP based on their End to End Delay.

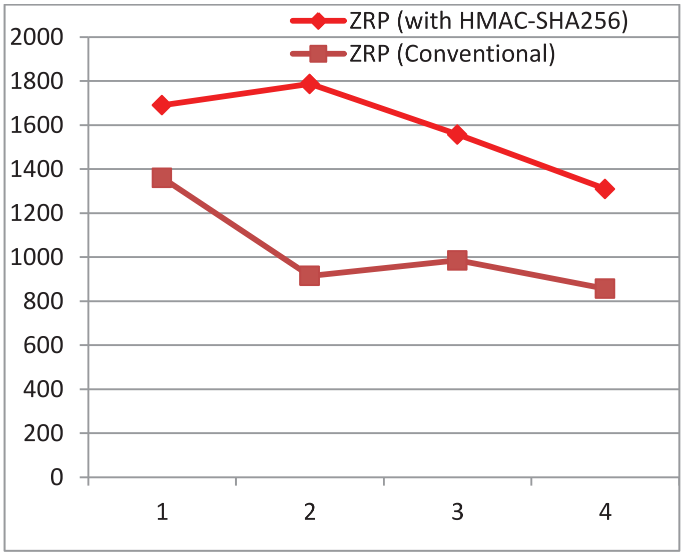

Figure 2: End-to-End Delay vs Zone Radius of ZRP and SZRP

B. ZRP Analysis with HMAC-SHA256 and Trust-Based System

With HMAC-SHA256 implemented into the ZRP patch in NS2, the next step is to incorporate the Trust-Based system in the ZRP for the prevention of DoS attacks. For this analysis, the simulation is done for different number of nodes from 10 to 50 and varying the zone radius from 1 to 5. As MANETs consist of mobile network, the pause time that defines the mobility is varied from 10s to 50s in steps of 10s. For the mobility, a scenario file is generated that uses a 'setdest' function which gives an output file with the required pause time for the analysis.

TABLE II
SIMULATION PARAMETERS

Source	3
Destination	45
Simulator	NS - 2.33
Protocol	ZRP
Type of Attack	Packet Dropping
Simulation Duration	50s
Simulation Area	1000M X 1000M
Propagation Model	2-Ray Ground Reflection
No. of Nodes	50
Channel	Wireless
MAC Protocol	IEEE 802.11
Antenna	Omnidirectional
Interface Queue Size	50 Packets
Mobility Model	Random Way Point
Pause Time	20s
Zone Radius	5
Number of Connections	90 CBR (TCP)
Malicious Nodes	5 , 10 , 15 , 20 , 25
Transmission Range	250m
Data Rate	2Mb

Figure 3 illustrates the Packet Delivery Fraction (PDF) in the network using ZRP protocol without and with Trust based systems. From the figure 3, the PDF obtained using SZRP is higher than conventional ZRP and as the number of malicious nodes increases the PDF decreases because of packet drops. We observed that the Packet Delivery fraction of the ZRP without trust when compared to that of with trust, the one with the trust based system performs better as it takes into consideration of the malicious nodes in the network. The initial PDF is never 100% as some packets are lost due to mobility. Thus the ZRP with trust rather than taking the shortest path also takes into consideration the behavior of the nodes.

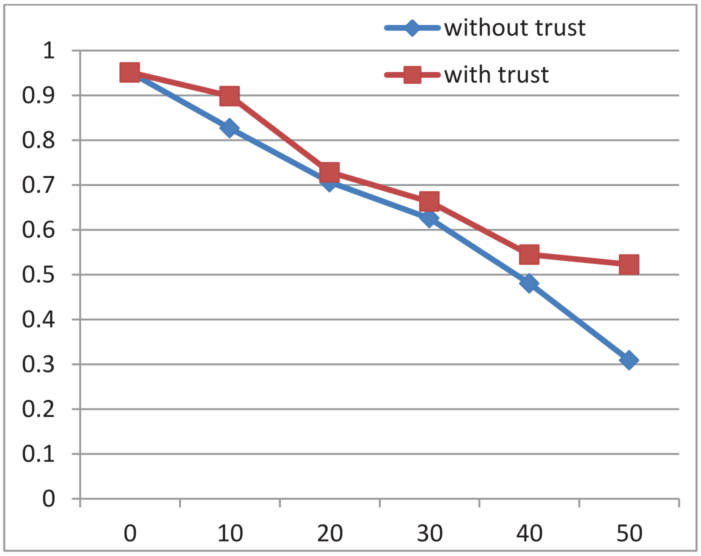

Figure 3: Packet Delivery Fraction vs Number of Malicious Nodes (%age)

The end to end delay for the trust based system increases as the time taken to traverse the same distance (in hops) increases as compared to the conventional ZRP without trust. Figure 4 illustrates the E2E Delay of the two systems.

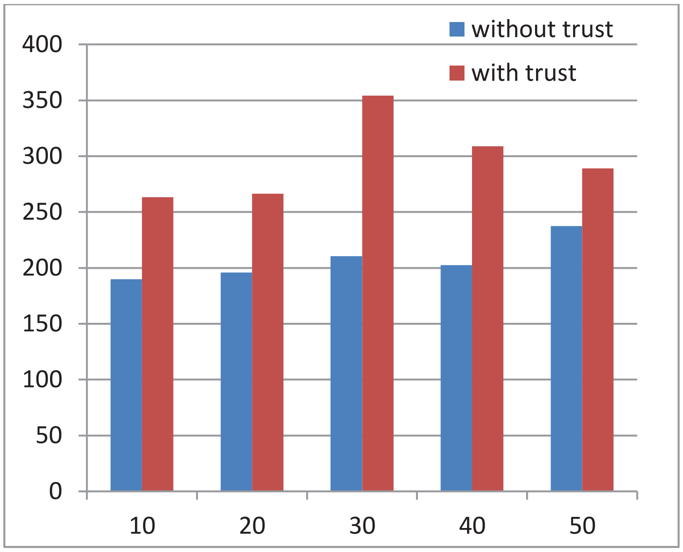

Figure 4: E2E Delay vs Malicious Nodes (%)

Figure 5 and Figure 6, illustrates the Throughput and Packet Delivery Fraction, respectively.

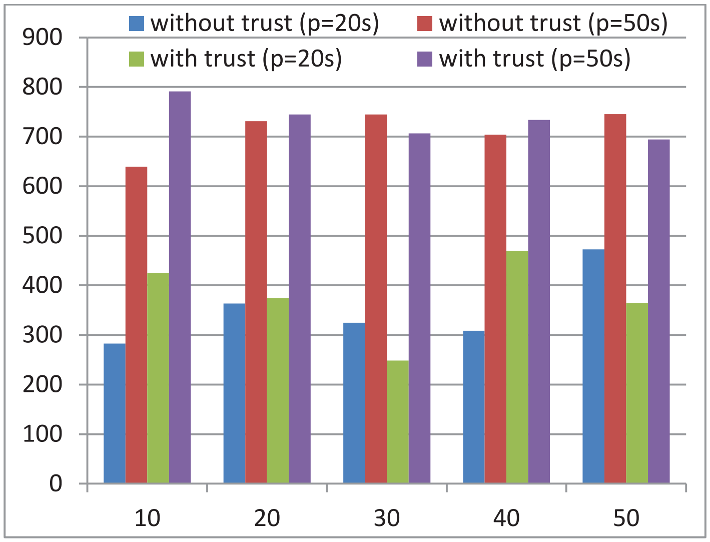

Figure 5: Variation of Throughput with Pause Time

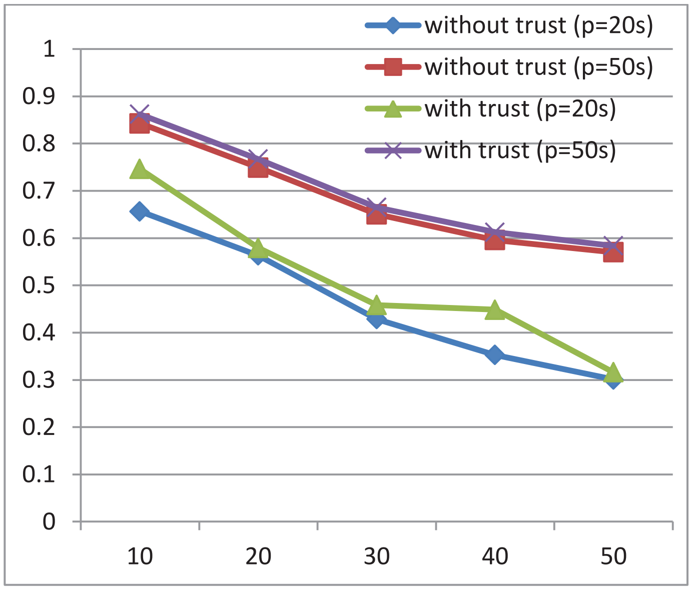

Figure 6: Variation of PDF with Pause Time in ZRP and SZRP

From the above results, with the increase of the pause time, the network gets more stabilized and thus the Throughput and the Packet Delivery Fraction increases but as expected, the pause time should decrease the end to end delay but in this case, there is an increase in that parameter which is because of the random way point mobility model used for the generation of the scenario file for doing the analysis. This causes the change in the initial co-ordinates of the node and their movement in the two cases with different pause time and hence causes the deviation from the expected result.

Figure 7 shows the simulation of analysis. The simulation shows the 'Malicious' nodes in an environment with total 30 nodes.

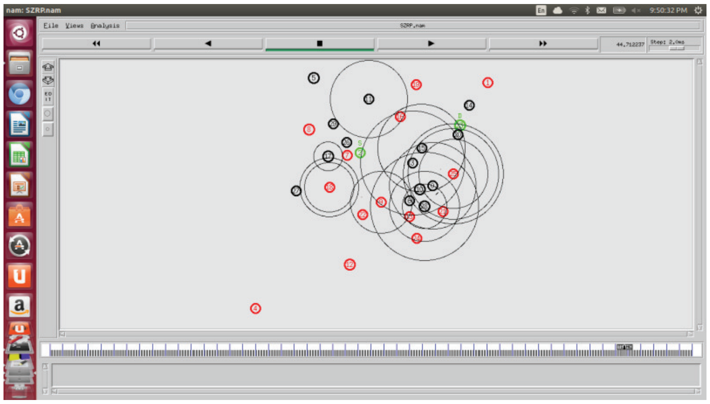

Figure 7: Simulation with Number of Nodes = 30

IV Conclusion And Futurescope

In this paper, the routing approach in mobile ad hoc networks from the security viewpoint is considered and analyzed the threats against ad hoc routing protocols and presented the requirements that need to be addressed for secure routing. Existing secure routing protocols for mobile ad hoc networks are either proactive or reactive in nature; hence are limited in their approach in terms of providing security across diverse networking applications. In this paper two techniques namely HMAC-SHA256 for providing data integrity along with authentication and Trust-Based system to make the network more secure by preventing Denial of Service attacks in the network are used.

In designing SZRP, carefully the inexpensive cryptographic primitives namely hash function (HMAC-SHA256) is fitted to each part of the protocol functionality to create an efficient protocol that is robust against multiple attacks in the network. The proposed protocol gives a better solution towards achieving the security goals like message integrity and message authentication, by taking an integrated approach of digital signature. Along with cryptography based solutions, a Trust Based solution is also implemented which is based on the behavior of the nodes.

The first part of the paper is implementation of HMAC-SHA256 on to the existing ZRP which provides us data integrity and authentication but at the expense of the increased processing delay. The other part being the implementation of the Trust Based system that considers the malicious nodes of the network and tries to avoid them as these nodes affects the Packet Delivery Fraction (PDF). The Trust Based system increases the PDF but at the expense of the increased End to End Delay. The simulations further show that as the malicious nodes percentage goes past 30%, the performance of the system degrades considerably. Furthermore, the mobility plays an important role while analyzing the network. If the pause time is increased, the mobility decreases that leads to more stable networks. Therefore, SZRP is an efficient way of discovering and maintaining routes in an open environment.

The future possible extension of our work may include employing additional feature to SZRP so that it can handle a scenario where the data is also confidential between the source and the destination and there are some safeguards against any attack to the data privacy (confidentiality). This implementation will increase the scope of the project to the military level operations where we need the security as well as privacy against the eavesdropping attacks. In addition one can implement a secure – key exchange mechanism so that multiple nodes can communicate in the network simultaneously in a secure manner without the prior knowledge to the secret key amongst the source 'S' and Destination 'D'. Further, a protocol can be devised as to make the nodes malicious in the network at random rather than defining the parameter our self.

REFERENCES

[1] Xing Fei; Wang Wenye, ―Understanding DoS Attacks in Mobile Ad Hoc Networks‖, MILCOM 2006, Oct. 2006, pp. 1 – 7.

[2] Bo Sun, Kui Wu, Yang Xiao, and Ruhai Wang, ―*Integration of Mobility and Intrusion detection for wireless ad hoc networks‖*, International Journal of Communication Systems,pp.695–721, 2007.

[3] Y. Zhang, W. Lee, and Y. Huang, ―*Intrusion Detection Techniques for Mobile Wireless Networks‖*, ACM Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[4] S. Al-Otaibi S, F. Siewe, "*Secure Routing Protocol Base on Secure Path in Ad hoc Wireless Networks*", IEEE International Forum on Computer Science-Technology and Applications IFCSTA 2009.

[5] **S .** Al-Otaibi , F . Siewe, "*Security of access in hostile environments based on the history of nodes in ad hoc networks*", IEEE the First Asian Himalayas International Conference on Internet AH-ICI 2009.

[6] Ali Hilal Mohamad, H. Zedan, A. Cau, ―*Security Solution for Mobile Ad Hoc Network of Networks (MANoN)‖*, IEEE Fifth International Conference of Networking and Services ICNS 2009.

[7] Esa Hyytiä and Jorma Virtamo, *"Random waypoint model in n-dimensional space"*, Operations Research Letters, vol. 33/6, pp. 567 – 571, 2005.

[8] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[9] C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.

[10] L. Zhou and Z. J Haas, "Securing Ad Hoc networks," IEEE Network Magazine, vol. 13, no. 6, December 1999.

[11] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer, 2008.

[12] Gabriel Montenegro and Claude Castelluccia, "Crypto-Based Identifiers (CBIDs): Concepts and Applications'" ACM Transactions on Information and System Security, February 2004.

[13] S Neelavathy Pari, Sbrish Jayapal and Sridharan Draisamy, "A Trust Security in MANET with Secure Key Authentication Mechanism", ICRTIT – 2012