IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 3 (Sep-Oct. 2012), PP 53-58
www.iosrjournals.org

Security in MANET based on PKI using fuzzy function

I.M.Hanafy[1], A.A.Salama[2], M. Abdelfttah[3,] Y. M.Wazery[4]
[1,2]*Math and computer science dept. Faculty of science, Port Said University, Egypt*
[3,4]*Information system dept., Faculty of computers & information, Banha University, Egypt*

Abstract: *In Mobile Adhoc Network the design of security model is a very critical and essential topic, this is due to the rapidly changing nature of this type of networks. Many other factors should be in consideration while handling mobile adhoc networks like the lake of infrastructure, bandwidth, etc. a security scheme is proposed based on Public Key infrastructure for distributing session keys between nodes. The length of those keys is decided using fuzzy logic manipulation for the discrimination between some of the attacks applied over this kind of networks. The proposed algorithm of Security-model is an adaptive fuzzy logic based algorithm that can adapt itself with the dynamic conditions of mobile hosts. Experimental results show that the use of fuzzy based security can enhance the security of mobile adhoc networks.*

Keywords: *MANET; Security; wireless; Communication; fuzzy; PKI; KNN*

I. Introduction

A Mobile Ad-hoc Network (MANET) is a collection of nodes that are self configuring (network can be run solely by the operation of the end-users). Nodes communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Each node in MANETs plays both the roles of routers and terminals. Such devices can communicate with another device that is immediately within their radio range or one that is outside their radio range not relying on access point[1]. A mobile ad hoc network is self-organizing, self-discipline and self-adaptive. The main characteristics of mobile ad hoc network are:

- Infrastructure-less: (Dynamic topology) Since nodes in the network can move arbitrarily, the topology of the network also changes.
- Bandwidth Limitations: The bandwidth of the link is constrained and the capacity of the network is also variable tremendously [2]. Because of the dynamic topology, the output of each relay node will vary with the time and then the link capacity will change with the link change.
- Power limitations: it is a serious factor. Because of the mobility characteristic of the network, devices use battery as their power supply. As a result, the advanced power conservation techniques are very necessary in designing a system.
- Security limitations: The security is limited in physical aspect. The mobile network is easier to be attacked than the fixed network. Overcoming the weakness in security and the new security trouble in wireless network is on demand [3].

A side effect of the flexibility is the ease with which a node can join or leave a MANET. Lack of any fixed physical and, sometimes, administrative infrastructure in these networks makes the task of securing these networks extremely challenging [4].

The rest of this paper is organized as follows; Some backgrounds are given in section 2. In section 3. Section 4 provides the proposed security mechanism. A comparison of the proposed mechanism with some of the current security mechanisms is provided in section 5. Section 6 provides the conclusion s and future work.

II. Preliminaries

2.1 MANETs

Adhoc is a Latin word, which means"for this or for this only" AdHoc Networks, as the name implies, are "meant to be" temporary in nature. The idea is to eliminate the BS completely. Imagine a scenario in a disaster relief operation Where in timely communication is a very important factor, the relief workers come in the area and without the need of any existing infrastructure, just switch on their handsets and start communicating with each other while moving and carrying out rescue work [5]. One main challenge in design of these networks is their vulnerability to security attacks. In this paper we provide an overview of security and ad hoc networks, and security threats applicable to ad hoc networks.

A wide range of military and commercial applications have been proposed for MANETs. For example, a unit of soldiers moving in the battlefield cannot afford to set up a base station every time they proceed to a new area. Similarly, setting up a communication infrastructure for a casual and spontaneous conference meeting among a small number of people cannot be justified financially [6].

Also robot based networks in which several robots work simultaneously to do gobs these are extremely difficult for human being (outer space discovery and mineral mining), Smart homes and another important application exists in what so called Vehicles Auto-Routing applications. Additionally, MANETs can be the perfect tool for a disaster recovery or emergency situation when the existing communication infrastructure is either destroyed or disabled.

In MANETs it is very important to address the security issues related to the dynamically changing topology of the MANET [7], these issues may be defined as:

1- **Confidentiality**. The primary confidentiality threat in the context of MANET is to the privacy of the information being transmitted between nodes, which lead to a secondary privacy threat to information such as the network topology, geographical location, etc.

2- **Integrity**. The integrity of data over a network depends on all nodes in the network. Therefore threats to integrity are those which either introduce incorrect information or alter existing information.

3- **Availability**. This is defined as access information at all times upon demand. If a mobile node exists, then any node should be able to get information when they require it. Related to this, a node should be able to carry out normal operations without excessive interference caused by the routing protocol or security.

4- **Authorization**. An unauthorized node is one which is not allowed to have access to information, or is not authorized to participate in the ad hoc network. There is no assumption that there is an explicit and formal protocol, simply an abstract notion of authorization. However, formal identity authentication is a very important security requirement, needed to provide access control services within the ad hoc network.

5- **Dependability and reliability**. One of the most common applications for ad hoc networks is in emergency situations when the use of wired infrastructure is infeasible. Hence, MANET must be reliable, and emergency procedures may be required. For example, if a routing table becomes full due to memory constraints, a reactive protocol should still be able to find an emergency solution.

6- **Accountability**. This will be required so that any actions affecting security can be selectively logged and protected, allowing for appropriate reaction against attacks. The misbehaviours demonstrated by different types of nodes will need to be detected, if not prevented. Event logging will also help provide non-repudiation, preventing a node from repudiating involvement in a security violation [8].

7- **Non-repudiation** Ensures that the origin of a message cannot deny having sent the message.

2.2 Public Key Security

The distinctive technique used in public key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message, not the same as the key used to decrypt it. Each user has a pair of cryptographic keys - a public encryption key and a private decryption key [9]. The provision of public key cryptography is widely distributed, while the private-decryption key is known only to the recipient. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The keys are mathematically related, but the parameters are chosen so that the determination of the private key of the public key is prohibitively expensive. The discovery of algorithms that can produce pairs of public / private key revolutionized the practice of cryptography in principle in mid-1970.
In contrast, symmetric key algorithms, variations of which have been used for thousands of years, uses a single secret key - that should be shared and kept private by the sender and receiver - for encryption and decryption. To use a symmetric encryption scheme, the sender and receiver must share the key securely in advance. Because symmetric key algorithms are almost always much less computationally intensive, it is common to exchange a key using a key exchange algorithm and transmit data using that key and symmetric key algorithm [10]. Family PGP and SSL / TLS schemes do this, for example, and therefore speak of hybrid cryptosystem.
The two main branches of public key cryptography are:
* Public Key Encryption: a message encrypted with the recipient's public key can be decrypted by anyone except a holder of the corresponding private key - presumably this will be the owner of that key and the person associated with the public key used. This is used for confidentiality [11].
* Digital signatures (Authentication): a signed message with the sender's private key can be verified by anyone with access to the sender's public key, which shows that the sender had access to the private key (and therefore likely to be the person associated with the public key used), and part of the message has not been tampered with. On the question of authenticity, see also the summary of the message [12].
The main idea behind public-key (or asymmetric) cryptosystems is the following:

One entity has (in contrast to symmetric cryptosystems) a pair of keys which are called the private key and the public key. These two parts of the key pair are always related in some mathematical sense. As for using them, the owner of such a key pair may publish her public key, but it is crucial that she keeps the private key only for herself. Let (sk, pk) be such a key pair where sk is the Secret private Key for node (A) and pk is the corresponding public key [13]. If a second node wants to securely send a message to (A) it computes C = encrypt(M, pk) where encrypt denotes the so-called encryption function which is also publicly known as shown in Figure 1.

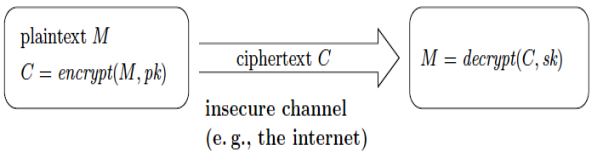

Figure 1: Asymmetric Key encryption / decryption

This function is a one-way function with a trap-door. In other words, the trap-door allows for the creation of the secret key sk which in turn enables Alice to easily invert the encryption function. We call C the ciphertext. Obtaining M from C can be done easily using the (publicly known) decryption function decrypt and A's private key (sk). On the other hand, it is much harder to decrypt without having any knowledge of the private key. As already mentioned, the great advantage of this approach is that no secure key exchange is necessary before a message is transmitted [14].

A central problem for the use of public key cryptography is the confidence (ideally proof) that a public key is correct, belongs to the person or entity claimed (ie, is "true"), and has not been altered or replaced by a malicious third party. The usual approach to this problem is to use a public key infrastructure (PKI), in which one or more third parties, known as certification authorities, certification of ownership of key pairs. PGP, as well as a certification authority structure, has used a general scheme, called the "web of trust" that decentralized public key authentication as a central mechanism, the replacement of individual supports the relationship between the user and the public key [15].

III. The proposed model for security

In this section, a Security algorithm applied to MANETs is presented. This algorithm may be viewed as a two stages: first a fuzzy model to decide the key length for the current session. Then the key distribution between nodes in MANET both stages are illustrated in the rest of this section.

3.1 Fuzzy model (Key Size Determination Function)

The security offered by the algorithm is based on the difficulty of discovering the secret key through a brute force attack. Mobile Status (MS) Security Level is the correlative factor being analyzed with three considerations:

(1) The longer the password, harder to withstand a severe attack of brute force. In this research the key lengths from 16 to 512 are assumed

(2) The quickest way to change passwords, more secure the mobile host. It is more difficult to decipher the key to a shorter time. A mobile host to change the secret key is often safer than a mobile host using a constant secret key.

(3) The neighbor hosts the mobile host has, the more potential attacker. I.e. the possibility of attack is greater. There are many other factors affecting the safety of mobile hosts, such as bandwidth. The security level of mobile hosts is a function with multiple variables and affected more than one condition.

Here a fuzzy logic system is defined . Inputs of the fuzzy logic system are the frequency of changing keys *(f)* and the number of neighbor hosts *(n)*. Output of the fuzzy logic system is the Security-Level of MS. It is assumed that the three factors are independent with each other. The relationship of them is as follows:

$$S \propto l \bullet f \bullet \frac{1}{n}$$ Formula 1

It means that the Security-Level of MH is in direct proportion to the length of the key and the frequency of changing keys, in inverse proportion to the number of neighbor hosts. The *S* value is updated by the fuzzy logic system. When the key length is short, the Security-Level of MH should be low; otherwise the Security-Level of MS should be high.

- The input fuzzy variable "the number of neighbor hosts" has three fuzzy sets—few, normal andmany. The membership function of *n* is illustrated in Figure 2.

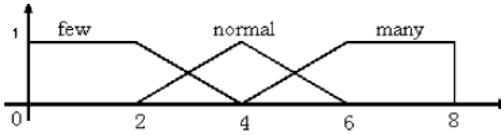

Figure 2: Membership function of fuzzy variable *n.*

- The input fuzzy variable "the frequency of changing keys" has two fuzzy sets—slow and fast. The membership functions of *f* is showed in formulation (2)

$$f = \begin{cases} slow & \text{the secret key is constant} \\ fast & \text{the secret key is variable.} \end{cases}$$ Formula 2

- The output fuzzy variable "the Security-Level of MS" has five fuzzy sets -lowest, low, normal, high and highest. It should be noted that modifying the membership functions will change the sensitivity of the fuzzy logic system's output to its inputs. Also increasing the number of fuzzy sets of the variables will provide better sensitivity control but also increases computational complexity of the system. Table 1 shows the rules used in the fuzzy logic system.

Input		Output
F	N	S
Slow	Few	Low
Slow	Normal	Lowest
Slow	Many	Lowest
Fast	Few	Normal
Fast	Normal	Low
Fast	Many	Low
Slow	Few	High
Slow	Normal	Normal
Slow	Many	Low
Fast	Few	Highest
Fast	Normal	High
Fast	Many	High

Table 1: the fuzzy system rules

The output of that system is then passed into will decide the number of bits used and the security level required for the current situation will follow the following fuzzy rules:

S is lowest : the number of bits is 16; **S** is low : the number of bits is 32;
S is normal : the number of bits is 64; **S** is high : the number of bits is 128;
S is highest : the number of bits is 256 or 512.

3.2 key distribution

Once the fuzzy function has decided the length of the session key based on its criteria the problem of key creation and distribution arises. The nature of NANET poses great challenges due to the lake of infrastructure and control over the network. To overcome such problems the use of PK scheme is used to distribute the key under the assumption that one node (let us say the first node that originates the network) is responsible for the creation of session keys. If that node is going to leave the network it must transfer the process of key creation to another trusted node in the network.

1- Each node sends a message (Session Key Request SKR) encrypted with its private key (that message contains a key request and a timer) to the key creator node which owns a table that contains the public key for each node in the network. Figure 3 (a) where the direction of the arrow's head denotes the private key used encryption is the originating node.
2- The key creator node simply decrypts the message and retrieves the request and the timer with one of the following scenarios occurs:

a. The timer was expired or the message is unreadable the message is neglected.
b. The timer is valid and the decryption of the message using the corresponding Public Key gives a readable request. The key creator node sends a message to that node containing the current session key. That message is encrypted two times first using the key creator's Private key(for authentication) then using the destination's public key Figure 3 (b). Where the direction of the arrow's head denotes the private key used encryption is the trusted node then with the destination node's Public Key.

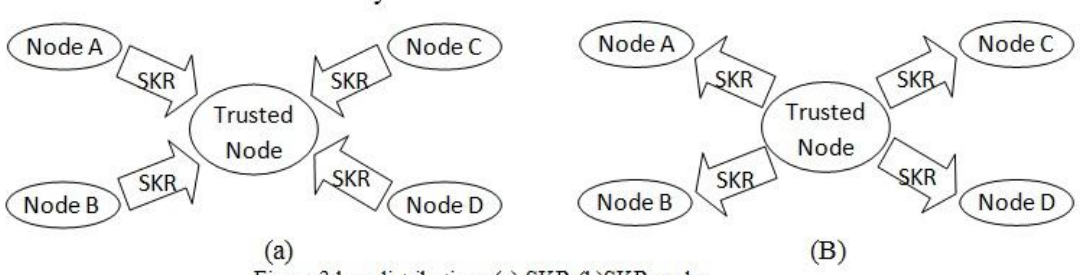

Figure 3 key distribution: (a) SKR (b)SKR reply

3- Any time the fuzzy model reports that the network condition changes; the key creator node sends a jamming message for every node currently in the network asking them to send a key request message.

4- Any authenticated node (including the Trusted node) on the network knowing the current session key can send messages either to every node or to a single node on the network, simply by encrypting the message using the current session key. .

IV. Experimental Results

In this research a new security algorithm for MANETs is presented, this algorithm is based on the idea of periodically changing the encryption key thus make it harder for any attacker to track that changing key. The algorithm is divided into two stages key size determination function and key distribution. In this section the set of experimental results for the attempts to decide the way for creating a more secured MANETs. These experiments are clarified.

4.1 Fuzzy vs. Non-Fuzzy Key size determination function:

The first type of experiments had taken place to decide the key size for the encryption process. To accomplish this job the ordinary mechanism of KNN is used as a non-fuzzy technique. Given the same parameters passed to the fuzzy and the non-fuzzy function the performance is measured with evaluation criteria are the average security-level and the key creation time.
The performance criteria are demonstrated in the following sections:

4.1.1 The Average security-level:

Average security level is measured for both techniques as the corresponding key provided how much strength given the number of nodes, the results are scaled from 0 to 5 these results are shown in table 2 and figure 4

No. nodes	25	50	75	100	125	150	175	200	225	250
Non-Fuzzy	2.6	2.1	2.5	2.2	1.5	1.7	1.4	2.3	2	1.5
FC	3.4	3.6	3.8	3.9	4	4	4	4	4	4

Table 2 ASL of fuzzy vs. non-fuzzy classification

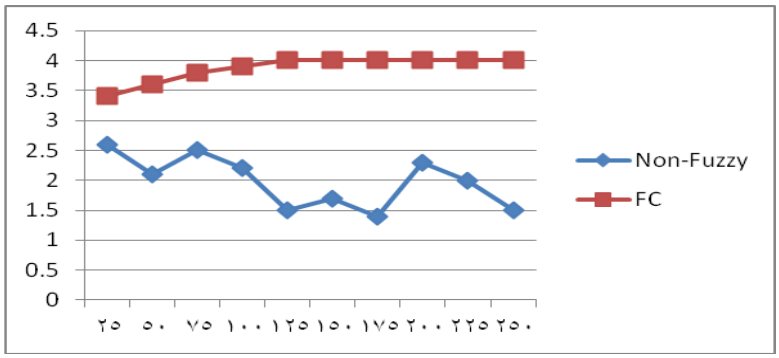

Figure 4: average security-level vs the number of mobile nodes

Figure 4 and table 2 shows the average security level with the number of mobile nodes between 25 and 250. As shown in the figure and the table, the average security-level of the Fuzzy Classifier (FC) is much higher than the average security-level of the non-fuzzy classifier, especially for many mobile nodes. This is an expected result since the fuzzy classifier adapts its self upon the whole set of criteria.

4.1.2 The key creation time:

The time required to generate the key in both cases are measured, the results are scaled from 0 to 1 and are shown in table 3 and figure5

No. nodes	25	50	75	100	125	150	175	200	225	250
Non-Fuzzy	0.95	0.93	0.95	0.96	0.96	0.96	0.96	0.96	0.96	0.96
FC	0.93	0.9	0.85	0.92	0.93	0.94	0.94	0.94	0.94	0.94

Table 3: KCR of fuzzy vs. non-fuzzy classifiers

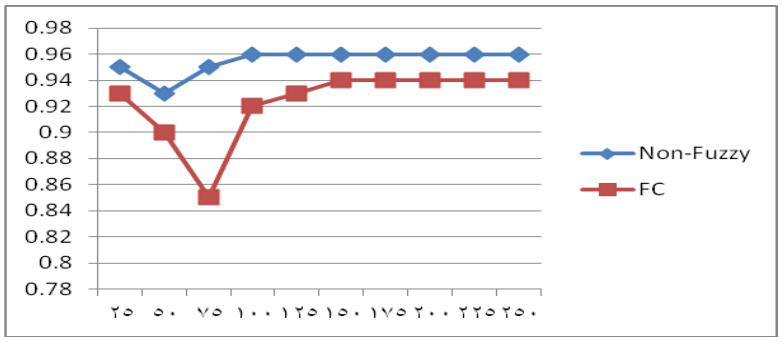

Figure 5: Key creation time vs the number of mobile nodes.

Figure 5 and table 3 shows the Key creation time with the number of mobile nodes between 25 and 250. The speed of Key creation is very high (mostly above 0.94) for all two techniques. However, the Non-fuzzy technique has some faster Key creation time than the Fuzzy Classifier, especially with few mobile nodes. The reason is that the smaller the number of nodes with the same amount of calculation the bigger the time taken.

4.2 PKI vs. non-PKI distribution

After the Key size had been determined via the Key size determination function the final problem is to distribute that key among nodes on the network. There were two approaches for the key distribution problem either PKI or non-PKI. In this subsection the results of applying PKI and non-PKI techniques is illustrated as applied in terms of security and processing time

4.2.1 Security

The PKI presents more overall security than ordinary non-PKI (single key) that is illustrated by applying both techniques over the network and recording the results regarding to the time required for an external attacker to break the session key. Table 4 and figure 6 shows that results under the assumption of using small public-private key pairs

No. nodes	25	50	75	100	125	150	175	200	225	250
Non-PKI	0.15	0.2	0.23	0.26	0.3	0.32	0.36	0.4	0.44	0.45
PKI	0.8	0.85	0.85	0.92	0.93	0.94	0.94	0.94	0.94	0.94

Table 4: security of PKI vs, non-PKI

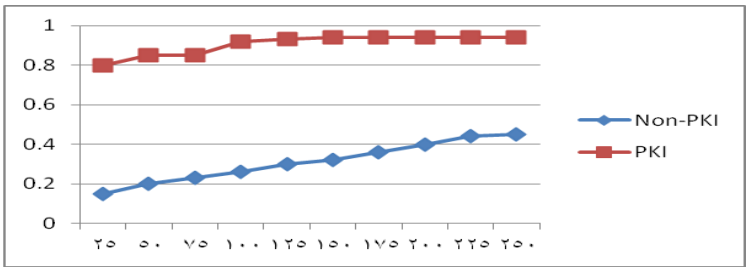

Figure 6: security of PKI vs., non-PKI

In graph and figure shows the huge difference in the security level provided by the PKI technique over the Non-PKI mechanism given the same experimental conditions.

4.2.2 Processing time

Another factor had been taken into consideration while developing the model that is time required to process the key and distribute it. Table 5 and figure 7 shows that results under the assumption of using small public-private key pairs

No. nodes	25	50	75	100	125	150	175	200	225	250
Non-PKI	0.3	0.32	0.35	0.37	0.4	0.44	0.47	0.51	0.55	0.58
PKI	0.2	0.35	0.5	0.6	0.68	0.75	0.83	0.87	0.93	0.97

Table 5 Processing time of PKI vs. non-PKI

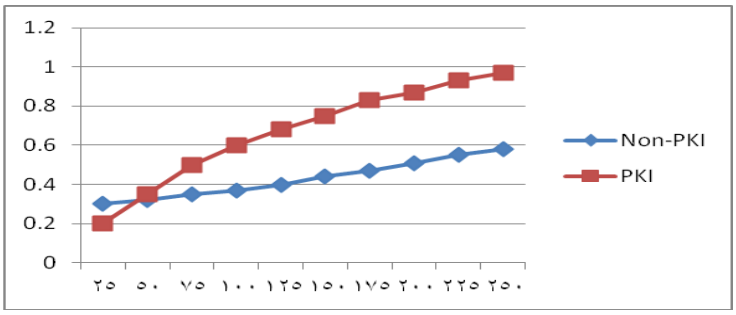

Figure 7: Processing time of PKI vs. non-PKI

Table 5 and the Figure 7 shows that Non-PKI techniques provides relatively small amount of processing time than PKI this due to the amount of modular arithmetic performed in the PKI mechanisms. However the difference in the processing time is neglectable comparing to the security level provided by the PKI under the same conditions

V. Conclusions

MANETs require a reliable, efficient, and scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. In this paper, we discussed the vulnerable nature of the mobile ad hoc network. The paper also covers the security attributes and the various challenges to the security of MANET. This paper also presents the new security mechanism which combine the advantages of both fuzzy classification and the public key infrastructure. Then the paper demonstrates the advantages of the proposed mechanism comparing to other existing mechanisms.

References

[1.] Balakrishnan, V. Varadharajan, U. K. Tupakula, and P.Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks". Proceedings of 4th IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, 2007.

[2.] AW. Stallings; "Cryptography and Network Security – Principles and Practice", 9th Edition; Prentice Hall 2010

[3.] Dr.A.Rajaram, S.Vaithiya lingam. " Distributed Adaptive Clustering Algorithm for Improving Data Accessibility in MANET". IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[4.] S. Balachandran, D. Dasgupta and L. Wang. " Hybrid Approach for Misbehavior Detection in Wireless Ad-Hoc Networks". Published in Symposium on Information Assurance, New York, June 14-15, 2006.

[5.] A.Rajaram, S.Palaniswami ." THE MODIFIED SECURITY SCHEME FOR DATA INTEGRITY IN MANET". International Journal of Engineering Science and Technology. Vol. 2(7), 2010, 3111-3119

[6.] C Balakrishnan, V. Varadharajan, U. K. Tupakula, and P.Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks". Proceedings of 4th IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, 2007.

[7.] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad-hoc and Sensor Networks," Algorithms and Protocols for Wireless Ad-hoc and Sensor Networks, A. Boukerche (ed.), Wiley & Sons, 2011.

[8.] K.Seshadri Ramana et al." Trust Based Security Routing in Mobile Adhoc Networks", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, pp 259-263.

[9.] Yan L. Sun, Wei Yu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", 2006 IEEE, pp305-317

[10.] Er. Banita Chadhaa, Er. Zatin Gupta," Security Architecture for Mobile Adhoc Networks" (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 9, 2011, pp 101 – 104

[11.] F. L. Bauer. Decrypted Secrets: Methods and Maxims of Cryptology. Springer, Secaucus, NJ, USA, 9th edition, 2009.

[12.] Dabrowski J. and Kubale M., Computer Experiments with a Parallel Clonal Selection Algorithm for the Graph Coloring Problem. IEEE International Symposium on Parallel and Distributed Processing (IPDPS 2008), 14-18 April, Miami, FL, USA, pp.1-6.

[13.] Rajaram A and Palaniswami S, "A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks", International Journal of Computer Science and Information Security, Vol. 6, No. 1,p.p 165 – 172, 2009.

[14.] Reza Azarderskhsh, Arash Reyhani-Masoleh." Secure Clustering and Symmetric Key Establishment in HeterogeneousWireless Sensor Networks". EURASIP Journal onWireless Communications and Networking .2011,

[15.] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," IEEE Transactions on Vehicular Technology, vol. 58, no. 8, pp. 4554–4564, 2009.