A Novel Approach to Secured Network Selection

A. K. Mohapatra
Asst Prof, Dept of IT
IGIT, GGSIP University, Delhi

Ankita Gulati
Dept of CSE, IGIT
GGSIP University, Delhi

Ruchika Luthra
Dept of CSE, IGIT
GGSIP University, Delhi

ABSTRACT

MANET (Mobile ad-hoc network) is a collection of mobile nodes that communicate over wireless links without having any pre-existing fixed underlying infrastructure. Their dynamically changing topology, lack of central administration and resource constraints makes them prone to security attacks. Quantifying security has always been a difficult task as there is no fixed measure of how secure is secure enough. Moreover, different people have different interpretations for security. In this paper, a security measurement framework for MANETS based on the five parameters CIANA (Confidentiality, Integrity, Authentication, Non-repudiation and Authorization) has been proposed. AHP (Analytic Hierarchy Process) and TOPSIS (Technique for order preference by similarity to Ideal solution) are then applied on the proposed models to select the most secure network amongst a set of heterogeneous networks.

General Terms

Network Security, Information security

Keywords

Confidentiality, Authentication, Integrity, Availability, Authentication, Security framework.

1. INTRODUCTION

MANETs (Mobile ad-hoc networks) are dynamic decentralized, self configuring, and infrastructure-less, wireless networks where a node can join and leave a network on its own as there is no central administration [3]. There is no disparity among the nodes. Each node acts both as a host and as a router to forward the packets to the peer nodes [8]. The topology keeps on changing. Open and shared nature of network, with the lack of central authority and the lack of clear line of defense makes it more prone to attacks and thus less secure [11][17]. Attacks in MANETs are classified as layer- specific attacks. Single layer attacks occur at a particular layer of the protocol stack and multi layer attacks can span multiple layers. The security solutions already available for the wired domain do not blend with the wireless domain. So, a solution is required that does not compromise the basic needs of CIANA (Confidentiality, Integrity, Authentication, Non-Repudiation, and Availability).

This work aims to devise a security framework for MANETs and thus estimate the security level among various heterogeneous networks. “When you can measure what you are speaking about and express it in numbers you know something about it,” wrote Lord Kelvin in 1883. “But when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind” [1], in this lies the idea and motivation behind this work. Quantifying security is a difficult task. It is very difficult if not impossible to devise a general solution or metric for estimation of security level of MANETs [11]. This work consists of the following sections-

Section 1: Introduction

Section 2: Security Models

Section 3: Security Framework

Section 4: Conclusion and Future Work

2. SECURITY MODELS

In this section, the security framework and its various elements are presented. While dealing with network security it must be ensured that the network satisfies the basic goals that an effective security paradigm must ensure.

In this framework, a security metric is represented as a tuple of 5 real numbers, each representing an aspect of the defined security and those aspects namely are Confidentiality, Integrity, Authentication, Non-Repudiation and Availability. Thus Security Metric has been defined as:-

<f1 (Confidentiality), f2 (Integrity), f3 (Authentication), f4 (Non-repudiation), f5 (Availability) >

The values in this five-topple indicate the measured strength of the Confidentiality, Integrity, Authentication, Non-repudiation and Availability of the system. In order to calculate the values of CIANA (as proposed to measure the security), 5 models are proposed, one for each factor. The proposed models are based on the Decomposition approach [1]:

1. As a subject of analysis, first find out or identify a set of security-related goal(s) for the system

2. The successive components that contribute to the success of the goal are also identified. For the success of the objective, these functions have to succeed

3. Examine if further decomposition is needed by examining the sub ordinate nodes. If yes, repeat the process with the subordinate nodes as current goals, and break them down to their functional components.

4. When none of the leaf nodes can be decomposed further or further analysis is no longer needed, terminate the decomposition process i.e. when the decomposition terminates, all leaf nodes should be measurable components which are independent of each other.

2.1 Model for Confidentiality

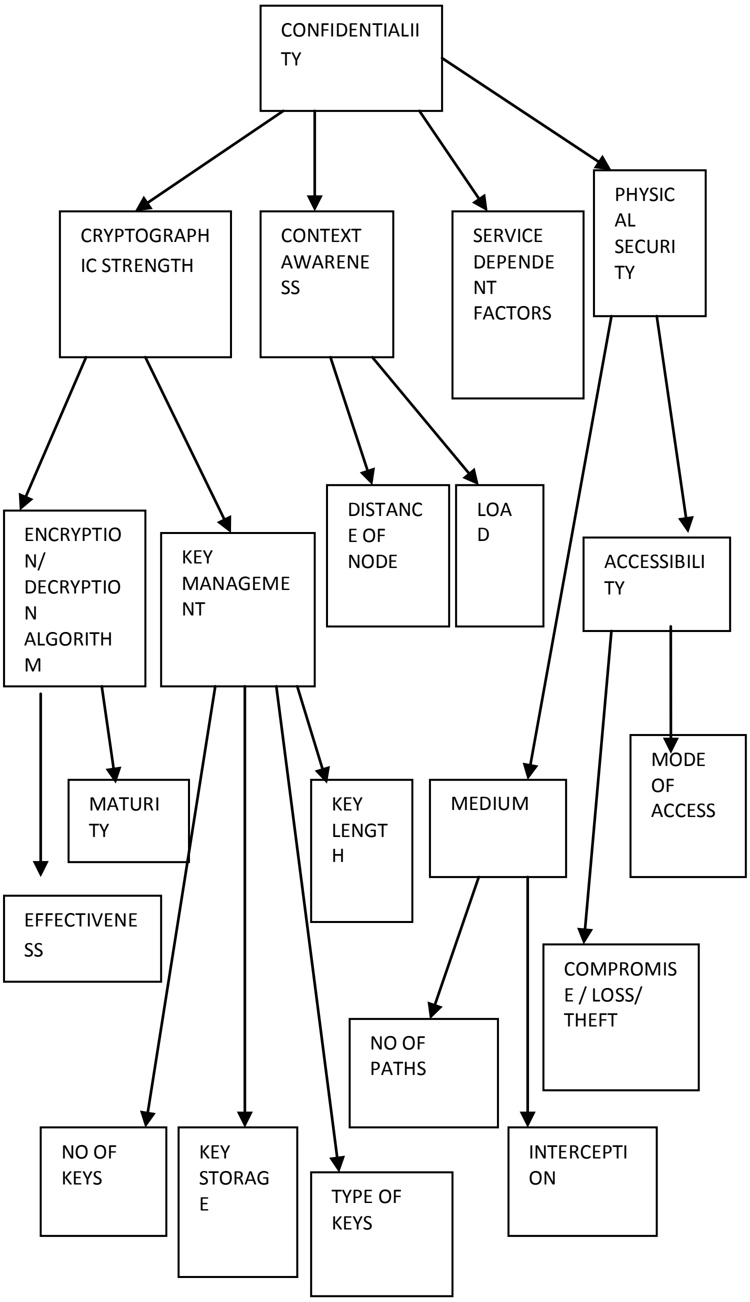

Fig 1: Model for Confidentiality

Confidentiality means the message or information is kept secure from unauthorized access/disclosure [4] [10].It ensures that secret information or data is never disclosed to unauthorized devices. Data confidentiality is the protection of transmitted data from passive attacks, such as eavesdropping. Sensitive information as in case of a battlefield requires confidentiality [13]. Confidentiality is decomposed into the components that affect the level in the network. The factors are-

2.1.1 Cryptographic strength:

Cryptographic strength is measured in the time and resources it would require to recover the plaintext. It is further dependent on the Encryption/Decryption algorithmic strength and Key Management. The Encryption/Decryption algorithm further depends upon its effectiveness and maturity. Key Management is affected by the Number of keys used in the session, how keys are stored (locally/remotely or both), types of keys (private/public), and key length. Small key length is susceptible to Brute force attacks.

2.1.2 Context awareness:

Context information like user's location and time also affect the level of confidentiality of the system. It is further dependent on the distance between the two communicating nodes and the traffic load present in the system. Distance represents the distance at which the nodes are placed relative to each other. Load in the network affects Confidentiality as the congestion in the network can cause the packets to be dropped.

2.1.3 Service dependent factors:

Service dependent factors can be thought of as the various factors affecting service quality. It can be related to service potential, service process or service result.

2.1.4 Physical security:

Physical security has been classified as the security of the medium and the accessibility mechanism. Medium is further is affected by interception and number of paths involved in the communication. Accessibility is further dependent on the mode of access, compromise/theft/loss. The mode of access can be nicest, broadcast or multicast.

2.2 Model for Integrity

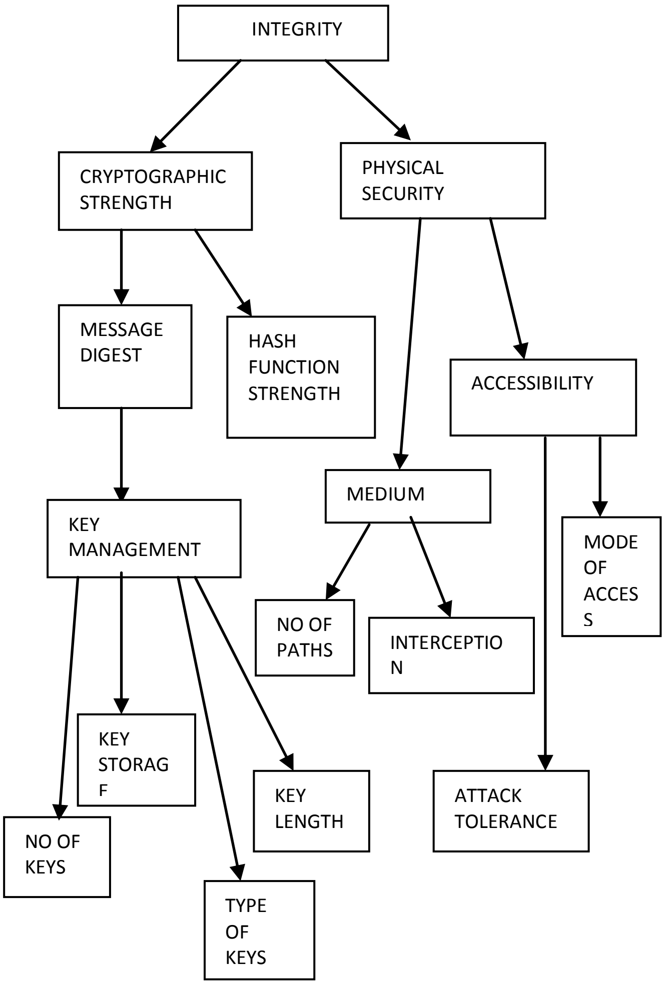

Fig 2: Model for Integrity

Integrity means message is unaltered during the communication between two parties [4].

It is the property that data has not been altered or destroyed in an unauthorized manner [10].Integrity is further affected by the following factors –

2.2.1 Cryptographic strength:

It is a measure of the expected number of operations required to defeat a cryptographic mechanism. It is further dependent on the hash function strength and its one way computability. To convert a variable length message into a fixed length message, a hash function is used. Also it is dependent on the message digest formed which is further dependent on key management. On obtaining the digest, we can encrypt it and send it to the receiver along with the original message. Key management is the creation, distribution and maintenance of a secret key. It determines how secret keys are generated and made available to both parties. Key management is affected by number of keys available during the entire session, key storage (local/remote/both), type of key (public/private) and key length. Small key length is susceptible to Brute force attacks.

2.2.2 Physical Security:

It depends upon the medium and accessibility. Medium is further affected by interception and number of paths involved in the communication. Accessibility is further dependent on mode of access and attack tolerance capacity.

2.3 Model for Authentication

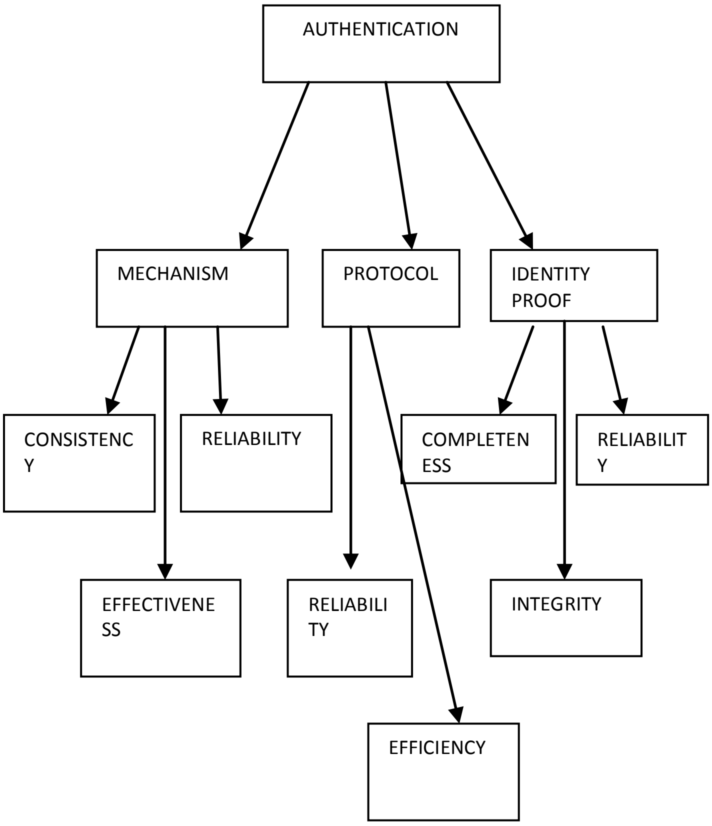

Fig 3: Model for Authentication

Authentication means that the message from the entity from which it was expected [4] [6].It enables a node to ensure the identity of the peer node it is communicating with. It means that it is impossible (or difficult) for an attacker to transmit in that channel, or at least to transmit without being detected by the legitimate participants [9].Authentication is probably the most important and complex issue in MANET because it is the bootstrap of the whole security system. Once authentication is achieved in MANET then confidentiality is just a matter of encrypting algorithm on the session by using keys [4]. The identification is based on credentials [2]. Authentication is dependent on the following components-

2.3.1 Mechanism:

Authentication mechanisms are encryption, message authentication codes(MAC) and digital signatures. The digital signature is a self organized and PKI authenticated by a chain of nodes without the use of a trusted third party [5]. It is further dependent on consistency, effectiveness and reliability of the mechanism used.

2.3.2 Protocol:

Authentication is dependent on the reliability and efficiency of the protocol used during communication in the network.

2.3.3 Identity Proof:

Identity proof is the evidence given by a credible person in order to prove his authentication. It is further affected by the completeness of proof, integrity and reliability of the proof and its provider.

2.4 Model for Non-Repudiation

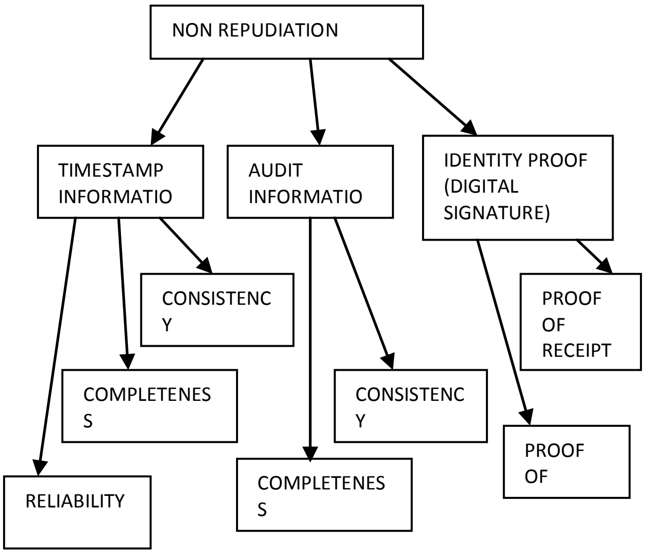

Fig 4: Model for Non-Repudiation

It ensures that the origin of a message cannot deny having sent/received the message [12]. The main mechanism used for this service is digital signatures [6].Non-repudiation is decomposed into the following components:

2.4.1 Timestamp Information:

If Non Repudiation is being used, secure timestamp services are required to attach a Coordinated Universal Time (UTC) timestamp to the secure audit log. It is about proving the existence of some information at some date and some time T. It is used to specify the time when the digital signature is made. This is needed to properly validate the signature. It is further decomposed into reliability, completeness and consistency of the timestamp involved. The essence of timestamp information is reflected in replay attacks. For example when a node sends an update request the attacker holds that request. The attacker can send this request to the server at a time when it is no more valid for the actual node [7].

2.4.2 Audit Information:

A secure audit log is also required for Non Repudiation. This log typically stores each business message with its digital signature and secure timestamp. An audit log is used to reconstruct the sequence of messages and other system events that have occurred during the exchange of business messages among trading partners. Audit information is characterized by completeness and consistency.

2.4.3 Identity Proof:

If the sender of a message ever denies sending it, the Non-Repudiation service with proof of origin can provide the receiver with undeniable evidence that the message was sent by that particular individual. If the receiver of a message ever denies receiving it, the non-repudiation service with proof of receipt can provide the sender with undeniable evidence that the message was received by that particular individual.

2.5 Model for Availability

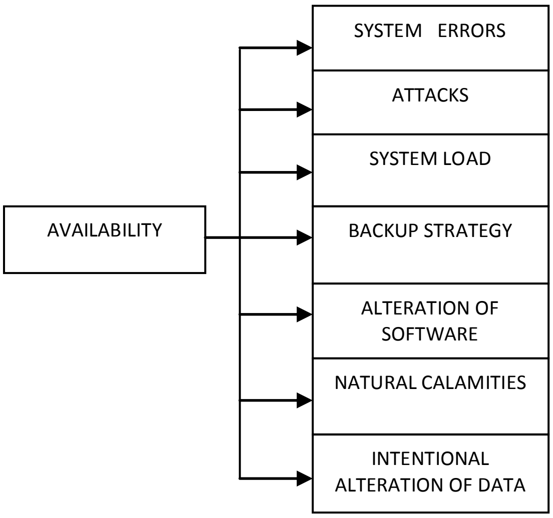

Fig 5: Model for Availability

Availability is the probability that a service request gets fulfilled. It is the property of being accessible and useable upon demand by an authorized entity. This probability can be determined through random samplings, statistics over a period of time, or specific testing. It ensures the survivability of network services despite denial of service attacks. [1] It is affected by the following components:-

2.5.1 System Errors:

Errors in the system can bring it to a halt, thereby affecting its availability.

2.5.2 Attacks

The injection of Trojans, viruses and worms also affect the availability of the system.

2.5.3 System Load:

If the load on the system is high, there is high chance of the requests not getting fulfilled.

2.5.4 Backup strategies

2.5.5 *Alteration of software:* It is possible that the software gets altered intentionally/unintentionally.

2.5.6 *Natural calamities:*

Natural disasters like earthquakes, floods etc. can bring the entire system under halt as the nodes may get lost or damaged.

2.5.7 Intentional alteration of data:

It is possible that the alteration of data is done intentionally in order to minimize the availability.

3. SECURITY FRAMEWORK

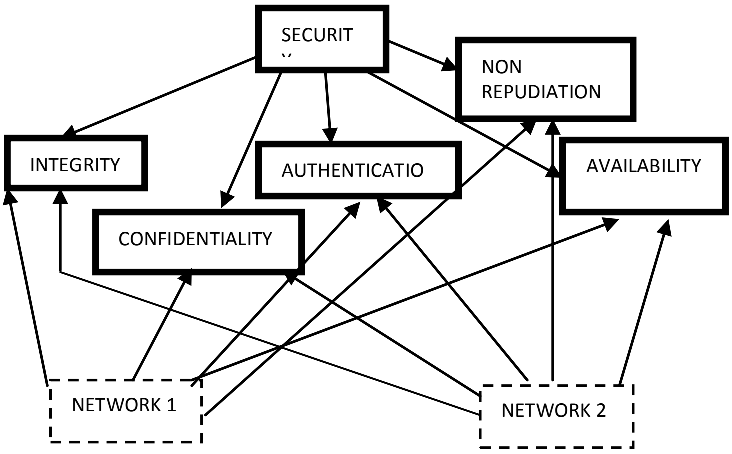

Fig 6: Security Framework

In this framework, Security is defined as a tuple of 5 attributes:

SECURITY = <f (Confidentiality), f (Integrity), f (Availability), f (Non-repudiation), f (Authentication)>

All these factors influence the security of a network. Hence, it is essential to address them effectively. In Section 2, various models for the above mentioned factors have been presented.

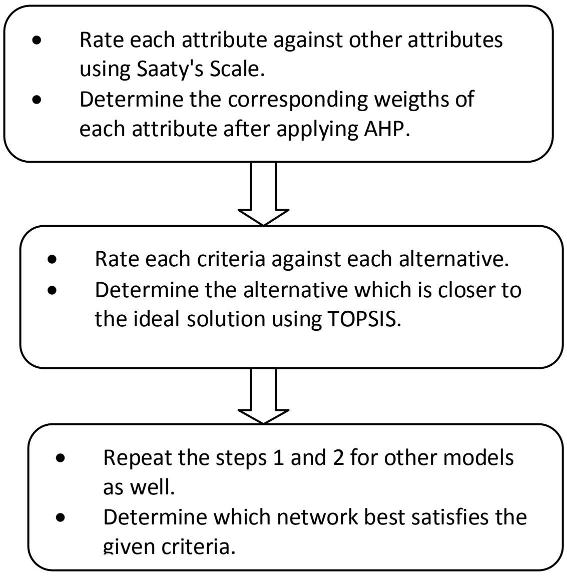
Rate each attribute against other attributes using Saaty's Scale.
Determine the corresponding weigths of each attribute after applying AHP.
Rate each criteria against each alternative.
Determine the alternative which is closer to the ideal solution using TOPSIS.
Repeat the steps 1 and 2 for other models as well.
Determine which network best satisfies the given criteria.

Fig 7: Proposed Approach for Network Selection

In order to select the best secured network amongst a set of heterogeneous/homogeneous networks, techniques of AHP [16] and TOPSIS [15] can be used. AHP [16] is used to determine the relative importance among the attributes in the various models and TOPSIS [15] is used to select the highly secured network that satisfies the user's criteria. TOPSIS [15] gives us the ranking of the various alternatives of networks in terms of their security.

4. CONCLUSIONS AND FUTURE WORK

An effective security paradigm must address the basic goals of security like Confidentiality, Integrity, Availability, Non-Repudiation and Authentication. A hierarchical approach has been followed in order to classify the attributes that are of utmost importance to these goals. The proposed security metric is a tuple of 5 attributes referred to as the CIANA (i.e. Confidentiality, Integrity, Authentication, Non-Repudiation and Availability). Each security goal has been decomposed into various factors and attributes that influence it. Considering that the attributes proposed in the above models are both quantitative and qualitative, measuring their exact value is a relatively difficult task. Saaty's rating scale can therefore be used to quantify the qualitative attributes. In the proposed scheme, AHP is intended to be applied to calculate the relative importance of one factor over the other followed by TOPSIS that selects the most secure network amongst a given set of networks based on the models proposed earlier. Future work is aimed at successful implementation of this framework that will incorporate the five models that have been proposed. This scheme will enable the user to select the network with high level of security amongst a set of networks that best satisfies the criteria.

5. REFERENCES

[1] Chenxi Wang, William A. Wulf, 1997. Towards a Framework for Security Measurement. In 20th National Information Systems Security Conference, Baltimore, MD, 522-533.

[2] Reijo Savola and Ilkka Uusitalo, 2006. Towards Node-Level Security Management in Self-Organizing Mobile Ad Hoc Networks. In AICT-ICIW '06 Proceedings of the Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services.

[3] Azzedine Boukerche, Begumhan Turgut , Nevin Aydin, Mohammad Z. Ahmad, Ladislau Bölöni, Damla Turgut , 2011. "A taxonomy of routing protocols in ad hoc networks". Journal of Computer Networks, Elsevier 2011.

[4] Muhammad Arshad Ali, Yasir Sarwar, March 2011.Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions. Master Thesis Computer Science.

[5] K.Selvavinayaki, K.K.Shyam Shankar, Dr. E. Karthikeyan, 2010. "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs". International Journal of Computer Applications, Volume 7– No.11.

[6] Zheng Wei, Meng Xin Jiang Li-Zheng, 2008. Security Architecture for Broadband Multicast Wireless Networks. In 4th International Conference on Wireless Communications, Networking and Mobile Computing.

[7] Sadaf Yasmin, Muhammad Yousaf, Amir Qayyum, 2010. Security Issues Related with DNS Dynamic Updates for Mobile Nodes: A Survey. In proceedings of the 8th International Conference on Frontiers of Information Technology.

[8] Jun-Zhao Sun, 2001. Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing. In proceedings of International Conference on Info-tech and Info-net.

[9] Dirk Balfanz, D. K. Smetters, Paul Stewart, H. Chi Wong, 2002. Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. In Proceedings of the 2002 Network and Distributed Systems Security Symposium (NDSS'02). San Diego.

[10] Reijo M. Savola, Habtamu Abie, 2009. Identification of Basic Measurable Security Components for a Distributed Messaging System. Third International Conference on Emerging Security Information, Systems and Technologies.

[11] Reijo M. Savola, Habtamu Abie, 2009. "On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks", Journal of Networks, Vol. 4, No. 7.

[12] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen .A security architecture for Mobile Ad Hoc Networks.

[13] Wenjing Lou, Wei Liu, Yuguang Fang, 2004. Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. In Conference of the IEEE Computer and Communications Societies.

[14] C. R. Dow, P. J. Lin, S. C. Chen, J. H. Lin, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference.

[15] C. Hwang and K. Yoon, 1981. Multiple Attribute Decision Making. In Berlin: Springer-Verlag.

[16] T.L. Saaty, 1980 .The Analytic Hierarchy Process. McGraw-Hill.

[17] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang.Security In Mobile Ad Hoc Networks: Challenges And Solutions. IEEE Wireless Communications, February 2004.