I. J. Computer Network and Information Security, 2013, 10, 44-50
Published Online August 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.10.07

Biometric based Security Solutions for MANET: A Review

Ajay Jangra, Shivi Goel
University Institute of Engineering and Technology, Kurukshetra, India
ajay.jangra@uietkuk.org, shivigoel2@gmail.com

Abstract — Mobile ad hoc networks are self organizing, infrastructure-less, low power networks, design to deploy bandwidth-shared radio channel communication and to work under vulnerable environment. Security is primary concern in MANETs and in order to achieve high security (confidentiality, integrity, authentication, availability and non repudiation), several techniques have been explored in which biometrics with cryptography or intrusion detection has gained a momentum in recent years. This paper critically reviews and investigates the present biometric based security models works for MANETs, and along with security challenges and direction of further research are proposed.

Index Terms — MANETs, security challenges, biometrics, cryptography, intrusion detection

I. Introduction

Mobile ad hoc network is wireless, infrastructure less, self organizing network with dynamic topology. MANET uses shared, error prone radio channel for communication. Due to the mobile nature of nodes there are frequent path breaks in MANETs. Nodes in MANET should have a transreceiver as well as routing/switching capabilities because they act as both host and router. Battery life and processing power are also major constraints in Ad hoc networks. Mobile ad hoc networks do not have central controller to coordinate the activities of nodes. Application domain of MANET includes:

Military Networks: The latest digital military fields demand strong and consistent communication in different forms. Mostly devices are deployed in moving military vehicles, tanks, trucks etc which can share information randomly among them. A simple example is shown in figure 1.

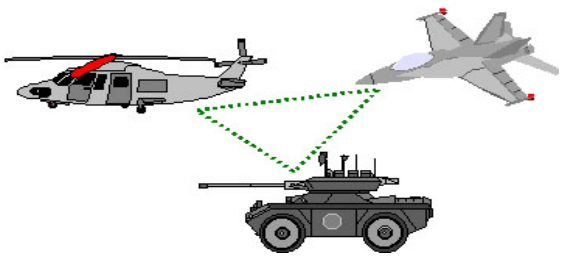

Figure. 1: Military Scenario

Sensor Networks: One more application of MANETs is the Sensor networks. It is a network which consists of a large number of devices or nodes called sensors, which sense a particular incoming signal and transmit it to appropriate destination node.

Automotive Applications: Automotive networks are extensively discussed currently. Vehicles should be enabled to communicate on the road with each other and with traffic lights forming ad-hoc networks of diverse sizes. This network will provide drivers with information about the road conditions, traffic congestions and accident-ahead warnings which help in optimizing the traffic flow.

Emergency services: Ad hoc networks are broadly being used in rescue operations for disaster relief efforts during floods, earthquakes, etc.

Security in wireless ad hoc networks has recently gained a momentum and became a primary concern in attempt to provide secure communication in hostile wireless ad hoc environment. Achieving security performances in wireless ad hoc environment is a challenging task because it has inherent vulnerabilities that are not easily preventable. Unlike wired network, any malicious node can attack from all directions and target on any node in MANETs. Attacks can be either passive like snooping or passive like information disclosure, session hijacking, repudiation or node impersonation and many more. Even the routing protocols of MANETs perform trust based computing, each node have to trust on neighbor node for communication. All this mean that MANET has no clear line of defense. All nodes are autonomous units and can move anywhere which mean that nodes with inadequate physical protection are receptive of being captured, compromised and hijacked. If the number of nodes are large in MANET, than it become difficult to track the compromised or malicious node.

A security protocol of ad hoc wireless networks should satisfy the requirements: *Confidentiality* ensures that the data can be understood by the destination node only. Though the intruder might get hold of the data being sent but he must not be able to derive the useful information through it. *Integrity* ensures that that the data is unaltered and untempered. *Authentication* ensures the identity of the node to which source is communicating. *Availability* ensures that network should remain operational all the time. *Non repudiation* ensures that both sender and

receiver cannot deny the participation in the communication.

The rest of the paper is organized as follows. Section II elaborates the security challenges in MANETs. Section III discusses some major attacks which violates the security constraints in MANETs. Section IV, V and VI presents three major techniques biometrics, cryptography and intrusion detection for security provisioning in MANETs. Section VII includes the detailed literature survey of biometric based security solutions with cryptography and intrusion detection. Section VIII concludes the work.

II. SECURITY CHALLENGES

Due to certain properties of mobile ad hoc network, designing a full proof security protocol for such networks is a very challenging task. There are several issues and challenges in security provisioning in MANETs as given below:

Bandwidth constraint: In MANETs shared radio channel is used for communication by each node which is limited for use. Each node has to use bandwidth optimally by keeping overhead as low as possible. Limited bandwidth availability imposes a constraint on nodes as they cannot apply complex security measures. Hence there is no secure boundary so any malicious node can enter into the network during the conversation and cause attacks like resource consumption so that other nodes (trusted) cannot utilize the bandwidth efficiently.

Trust based computing: MANET works on trust computing and on node Corporation. As any node whether normal, compromised or malicious can enter into the network at any point, it is not possible for any node to keep updated information about the nature of node, hence for routing, each node have to trust on its neighbor. Sender has to trust on its neighbor nodes in order to communicate with the desired destination. Hence it is difficult to derive the security constraints over the network without defining the level of trust of the participating nodes.

Dynamic routing and topology: Every node is independent and can move anywhere and hence the network topology in an ad hoc wireless network is highly dynamic. Due to mobile nature of nodes in MANET, applying fixed solution on network is a difficult task because the image of network changes randomly and hence the security requirements of that system.

Resource constraint: Due to small size, portable and compact nature of devices in MANET, there are limited resources and low computation power. Hence using complex security algorithms in MANET is a difficult task.

Distributed working approach: As there is no centralized authority in MANET, distributed approach is followed where responsibilities are shared over the network. Hence applying security methods in distributed method is also a challenging task *Insecure working environment:* Mobile ad hoc networks are mainly implemented in insecure environment like battlefield conditions, search and rescue conditions etc where it is difficult to identify malicious or compromised node.

III. ATTACKS

Attacks on MANET can be broadly classified into two broad categories namely Passive and Active attacks. Passive attacks do not disturb the normal functioning of network but it violates the confidentiality of the network. Detection of passive attacks is very difficult as they do not affect the functionality of network. In order to overcome this problem, powerful encryption mechanism should be implemented on the network. On the other hand, an active attack tries to alter or destroy the information which is being transmitted over network. Active attacks are further classified into four groups: *Dropping Attacks:* Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point [1]. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not. *Modification Attacks:* Sinkhole attacks are the example of modification attacks. These attacks modify packets and disrupt the overall communication between network nodes. In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks. *Fabrication Attacks:* In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages. *Timing Attacks:* In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

Some attacks are defined below:

Eavesdropping

Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. The information may include private key, public key, location or passwords of the nodes. Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap.

Malicious Behavior of nodes

The main aim of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes. Attacks of such type are fall into following categories. *Denial of Service (DoS):* These types of threats produced a malicious action with

the help of compromised nodes that forms severe security risks. In the presence of compromised nodes, it is very difficult to detect the compromised routing. The compromised route appears like a normal route but leads to severe problems. For example, a compromised node could participate in the communication but drops some packets which lead to degradation in the quality of service being offered by network. *Attacks on Network integrity:* Network integrity is an important issue, in order to provide secure communication and quality of service in network. There are so many threats which exploit the routing protocol to introduce wrong routing information. *Misdirecting traffic:* A malicious node advertises wrong routing information in order to get secure data before the actual route. These nodes receive information that was intended for owner of the address. A malicious node may advertise fake route request, so that other nodes will then direct route replies to the node. *Attacking neighbor sensing protocols:* malicious nodes advertise fake error messages so that important links interface are marked as broken. This will result in decrease in network throughput and quality of service.

Session Hijacking

Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc) and other information from nodes. Session hijacking attacks are also known as address attack which make affect on OLSR protocol.

Repudiation attacks

Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services

Sybil attack

In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called Sybil nodes. A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. Various effects due to presence of Sybil attacks are:

- In the presence of Sybil nodes in network, it may make difficult to identify a misbehaving node.
- Sybil attacks prevent fair resource allocation among the nodes in network.
- In certain application, sensors can be used to perform voting for decision making. Due to presence of duplicate identities the outcome of voting process may vary.
- Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in network.

Wormhole Attack

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes [2, 3]. When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the attack could prevent the discovery of any routes other than through the wormhole. If there is no defense mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes.

Although there are many security issues, confidentiality and authentication is core requirement. Several research works has been done in this field. Cryptography, biometrics and intrusion detection techniques are widely implemented and proved to be successful in ad hoc conditions in recent years.

IV. BIOMETRICS

Biometrics is becoming an increasingly popular method of identifying unique human characteristics as a mean of authenticating an individual's identity. The science of biometrics is ultimately based on analysis of distinctive physical traits such as fingerprints and retinal scans, as well as personal characteristics such as physical, biological patterns. Biometrics provides some possible solution to authentication used in MANETs since it has direct connection with user identity and need little user interruption. For tactical MANETs in hostile environments where chances of node capture are high, it is important to verify the presence of authentic user continuously. Each biometric technique has its own strengths and weakness. Also if once biometric is compromised, it is lost forever and possibly for every application where it is used.

It is possible that data obtained during biometrics enrollment may be used in ways for which the enrolled individual has not consented. For example biometric security that utilizes and employee's DNA profile could also to screen for various genetic diseases or other undesirable traits. Biometrics devices consist of a reader or scanning device, software that converts the gathered information into digital form and a database that stores the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data in the database.

V. CRYPTOGRAPHY

In order to achieve confidentiality and integrity in networks, cryptography is mainly used. Cryptography means secret writing. The original message called plain text is transformed into coded form called cipher text using a key which is a number or set of numbers.

There are two types of cryptography, symmetric key and asymmetric key. In symmetric key algorithm, the same secret key is used by both the sender and receiver for encryption and decryption respectively. The key is shared over the network. Whereas in asymmetric key algorithms, there are two keys: a private key and a public key. Private Key is kept by the receiver and public key is announced over the network. If sender wishes to communicate with the receiver he uses the public key of the receiver for encryption, on receiver side the private key is used for decryption.

VI. INTRUSION DETECTION SYSTEM

Intrusion detection [4] involves capturing audit data and reasoning about the evidence in the data to determine whether the system is under attack. Based on the type of audit data used, intrusion detection system can be categorized as network based and host based. A network based normally runs at the gateway of the network and captures and examines network packets that go through hardware interface. A host based IDS rely on system audit data to monitor and analyze the events generated by programs or users on the host. In the system aspect, individual IDS are placed on each and every node. Each IDS node runs independently and monitors local activities. If anomaly is detected in local data or data is inconclusive and border search is warranted, neighboring IDS will corporately participate in global intrusion detection actions. These individual IDS agents collectively form the IDS system to defend the wireless ad hoc network.

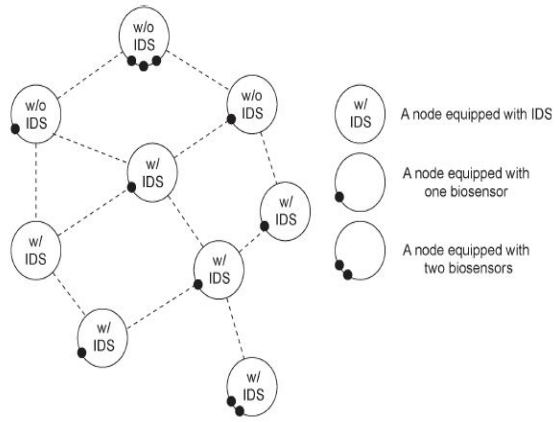

Figure 2: MANET having Nodes Equipped with IDS and Biosensors

A few research works has been done in the field of data security in MANETs implementing biometrics with cryptography and intrusion detection systems are briefly summarized. Typically framework of MANETs with biometric devices or biosensors and intrusion detection IDS would be as shown in figure 2

VII. LITRATURE SERVEY

Optimal biometric based continuous authentication in mobile ad hoc networks

In 2007, Jie Liu et al. [5] proposed optimal biometric based continuous authentication in mobile ad hoc networks which rely on multimodal biometric system. It adopts a centralized approach where biometric traits are kept on a secured system. It checks for authentication at discrete time intervals. Therefore biometric traits do not need to be acquired simultaneously. The time axis is divided into slots of equal duration which corresponds to the time interval between two continuous authentications. POMDP and relevant algorithms can be used to optimally pick a biosensor for authentication at each time instant and to balance the tradeoff between biosensor cost and estimation errors.

Under this model, there is no direct involvement of device as decision will be based on the outcome of biosensors. It focuses on user to device authentication which authenticate that device is in right hands.

Intrusion detection and continuous authentication in mobile ad hoc networks

Guaranteeing authentication is not the only solution to security because it cannot eliminate the intrusion of malicious node which can launch denial of service or disrupt the routing mechanism by generating error routing messages. Jie Liu et al. [6] proposed a two level protection model for MANET which includes two complementary classes of approaches to protect high security mobile ad hoc networks: prevention based approaches such as authentication and detection based approaches such as intrusion detection. As biometric have direct connection with the identity of user, it is used for user to device authentication. Second, intrusion detection system helps to identify malicious activities. IDS continuously or periodically monitor the current subject activites, compare them with stored normal profile and initiate the proper responses. This paper provides a framework for multimodal biometric system emphasing on re authentication which will be initiated at every time instant, IDS is continuously monitoring the system. It is assumed that continuous authentication system is equipped with multiple biosensors. Altogether if there are L sensors in the system, it assumes that only one sensor (either a re-authentication or IDS) will be chosen at one time instant.

There are several drawbacks of this system, firstly performing continuous authentication and intrusion detection may lead to security information leakage to an adversary monitoring malicious nodes. Second, continuous intrusion detection and authentication may consume a large amount of energy which is a concern for energy constraint devices in MANETs.

Optimal combined intrusion detection and biometric based continuous authentication in high security mobile ad hoc networks

To overcome the drawbacks of previous models, in 2009, Jie Liu et al. [7] proposed optimal combined intrusion detection and biometric based continuous authentication. Distinct features of the scheme proposed in this paper are:

- It can optimally control the activation of IDS.
- It can optimally control whether or not to perform authentication and which biometric to use to minimize usage of system resources
- Both IDS and authentication system will share information with each other to obtain efficient mechanism for providing security.

Although it eliminates the drawback of extensive consumption of resources due to continuous authentication and intrusion detection, but still it is a centralized scheme in which a central controller is needed to schedule authentication and intrusion detection which is not suitable for MANETs.

Distributed combined authentication and intrusion detection with data fusion in high security mobile ad hoc networks

Shengrong Bu et al. [8] proposed a distributed scheme of combining intrusion detection and continuous authentication. The system decides whether or not a user authentication is required and the decisions are made in fully distributed manner by each authentication device and IDS. As there is no centralized point, hence it is very important to detect the security state of each node. It is cluster based technique. More than one biosensors and IDS have to choose for detecting state in their local neighborhood at each time slot. Then it is the responsibility of chosen node to broadcast the detected information from optimal scheduling of authentication and intrusion activities, and these messages are digitally signed by their private keys. Based on the received information, each node will calculate the security state of other nodes. In each cluster above steps are carried out.

In order to obtain the security state of network, a chosen neighbor observes the node's behavior and accesses its security state. These observation values are then combined and decision about the security state of the node is made. In this paper, Dampster-shafer theory for data fusion is used. Since each device in network has measurement and estimation error, hence more than one device has to be chosen and observations can be fused to increase accuracy.

Efficient secure multimodal biometric fusion using palm print and face image

Nageshkumar et al. [9] presents a novel fusion strategy for personal identification using face and palm print biometric at the feature level fusion scheme. This paper presents a new method called canonical form based on PCA, which give better performance and better accuracy for both traits. The matching score for both traits is calculated by Euclidean distance. The modules based on individual traits returns an integer value after matching the templates and query feature vectors. The final decision is made by comparing the obtained score with threshold value stored at decision module.

Unimodal biometric encryption key

In order to provide confidentiality, integrity and authentication, Hiteishi Diwanji and J.S. Shah [10] proposed unimodal biometric encryption key method. In this paper with unimodal biometric fingerprint, 48 bit encryption key is generated for symmetric key encryption algorithm DES. The feature set is extracted from fingerprint, 2*16 matrix is generated. Crossover is performed on both the rows to generate 48 bit key which is difficult to generate for any cryptanalysis. This ensures confidentiality and integrity. For authentication digital signature is used.

As common to symmetric key algorithm, key should be shared prior to communication, but this scheme suggests the generation of key on both sides (sender and receiver) with the same formula, so stealing of key is not an issue.

This scheme withstands all the cryptanalysis attack because every time different feature set is used so cryptanalysis will not be able to find out the key even if intruder has got cipher text-plaintext pair.

Cryptographic key generation from multiple biometric modalities: Fusing minutiae with Iris feature

A Jagadeesan et al. [12] proposed a multimodal biometric cryptosystem where volatility of user's unique biometric traits is integrated into a generated key. It focuses on fusion of fingerprint and iris features at feature level because integration at this level is expected to provide fine recognition output. Steps involves extraction of minutiae points from fingerprint, extraction of features from iris then feature level fusion and then generating cryptographic key from fused features.

In order to extract minutiae points from fingerprints, the image of fingerprint is first enhanced using sliding neighborhood operations. It is based on local statistics and then region of interest is extracted for which the image is divided into non overlapping 16*16 sizes of blocks. Block is filled with ones only if resultant value of standard deviation of gradients exceeds the threshold value. After the extraction of ROI, the orientation field of image is to be estimated for which gradient based methods are used. The enhanced fingerprint image is used for the process of minutiae point extraction.

In order to extract features from iris, first iris segmentation is done in order to define the effective image region. The image is first fed as input to the canny edge detection algorithm that produces the edge map of iris image for boundary estimation. The exact boundary of pupil and iris is located from the detected edge map using the Hough transform and after that eyelids and eyelashes are isolated. Iris normalization is done using Daugman's rubber sheet model. The two set of features are then fused to obtain the multimodal biometric template that can carry out biometric authentication. And then K-bit cryptographic key is generated. This modal

enhances the security of the proposed approach by incorporating the complexity of factoring the large numbers as keys.

A genetic based non invertible cryptographic key generation from cancelable biometric in MANET

Manisha Mehta et al. [11] proposed cryptographic key generation from the cancelable fingerprint.

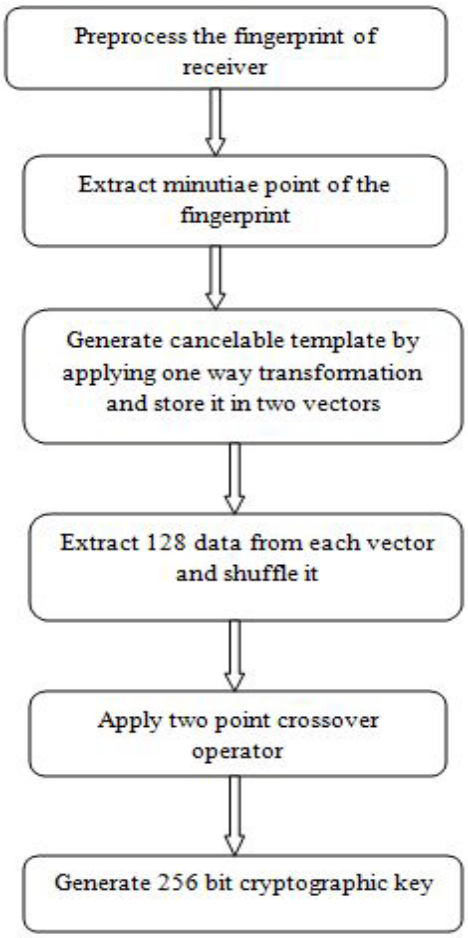

Figure 3: Process Diagram

To randomize the key two point crossover genetic operator is applied. It is assumed that face images and fingerprint images of group members are stored in database. The minutiae points are generated from the receiver fingerprint and transformed into cancellable template, two point crossover genetic points is applied and noninvertible key is generated. The sender's watermarked face image attached to data and encrypted using generated cryptographic key. At receiver side, reverse process take place. Receiver's fingerprint is used for decryption. The sender's face is extracted and watermarked image checked for authentication. This model provides confidentiality by implementing one way transformed function, it also provide authentication by using watermarked face biometric. It also provides integrity, as by the property of one way transform it is computationally infeasible to modify the cipher text by attackers. But maintain the database of biometric traits of all trusted users is difficult task and because of distributed nature of MANET, it becomes vulnerable also. The process diagram is shown in figure 3.

VIII. CONCLUSIONS

Although MANET is a very promising technology, challenges in security is slowing its development and deployment. Traditional security mechanisms are not sufficient for the nodes moving in a hostile environment with relatively poor physical protection. Several techniques are proposed in this section implementing biometric with cryptography or intrusion detection system which provides secure alternative for communication over network. But still these models are not too much efficient and robust so that they can be applied on real conditions effectively. Fingerprints can be forged and collecting and matching face prints is time consuming and complex. Veins and Vein patterns are yet not explored too much for MANETs. Some areas like pattern recognition in MANETs, securing and maintaining the biometric database in MANET, combining secure routing with authentication process, designing efficient cryptographic algorithms for MANETs and secure collection and maintenance of up to date audit data in intrusion detection system are still to be explored efficiently.

REFERENCES

[1] Panagiotis Papadimitratos and Zygmunt J. Haas. "The handbook of Mobile Ad Hoc Networks",CRC Press, Inc. Boca Raton, FL, USA, 2003.

[2] Pradip M. Jawandhiya, Mangesh M. Ghonge. "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, 2010.

[3] K.P. Manikandan, Dr. R .Satyaprasad, Dr. Rajasekhararao. "Analysis and Diminution of Security Attacks on Mobile Ad hoc Network", IJCA Special Issue on "Mobile Ad-hoc Networks "MANETs, 2010.

[4] Yongguang Zhang and Wenke Lee. "Intrusion Detection in Wireless Ad Hoc Networks" in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000), August 6–11, 2000.

[5] Jie Liu, F. Richard Yu, Chung-Horng Lung and Helen Tang. "Optimal Biometric-Based Continuous Authentication in Mobile Ad hoc Networks" in Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007) .

[6] Jie Liu, F. Richard Yu, Chung-Horng Lung and Helen Tang. "A Framework of Combining Intrusion Detection and Continuous Authentication in Mobile Ad Hoc Networks" in IEEE Communications Society, 2008.

[7] Jie Liu, F. Richard Yu, Chung-Horng Lung and Helen Tang. "Optimal Combined Intrusion Detection and

Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks" in IEEE transactions on wireless communications, vol. 8, no. 2, February 2009.

[8] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang. "Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks" in IEEE transactions on vehicular technology, vol. 60, no. 3, March 2011.

[9] Nageshkumar.M, Mahesh.PK and M.N. Shanmukha Swamy. "An Efficient Secure Multimodal Biometric Fusion Using Palm print and Face Image" in IJCSI, International Journal of Computer Science Issues, Vol. 2, 2009.

[10] Hiteishi Diwanji and J.S. Shah. "Enhancing Security in MANET through Unimodal Biometric Encryption Key" in IEEE, December 2011.

[11] Manisha Mehta, Hiteishi Diwanji, Jagdish S Shah. "A Genetic Based Non-Invertible Cryptographic Key Generation from Cancelable Biometric in MANET" in IJCTA, Nov-Dec 2011.

[12] A. Jagadeesan, T. Thillaikkarasi, Dr. K. Duraiswamy. "Cryptographic key generation from multiple biometric modalities: Fusing minutiae with Iris feature" in International Journal of Computer Applications, June 2010.

Dr. Ajay Jangra (*03rd Nov 1979, PhD, M.Tech, B.Tech, MBA(IT) & LLB**) Having rich teaching experience of more than 10 years and presently working as Assistant Professor in CSE department, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, INDIA. He has completed B.Tech. (Electronics and Communication Engineering) in 2001, M.Tech. (Computer Engineering) in 2004 with honours, and MBA (Information Technology) in 2008. Author has received PhD in 2011 in the area of Mobile Ad-Hoc and Wireless Sensor Networks and presently pursuing LLB in (evening session). He has published 52 research papers in reputed international journals/conferences, and 20 research papers in national level journals/ conference. His area of interest is smart sensors, Ad-Hoc & sensor networks, data communication& advance networks, High performance Mobile, grid & cloud computing etc.

Shivi Goel received her B.Tech. in computer science and engineering with honours in 2012. Currently she is pursuing M.Tech in computer engineering at University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, INDIA. Her field of interest is biometrics, cryptography and mobile ad hoc networks.

