International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 384 – 391

Biometric Based Intrusion Detection System using Dempster-Shafer Theory for Mobile Ad hoc Network Security

[1] Dr. Ramalingam M., [2] Dr. Prabhusundhar P, [3]Dr. Thiagarasu V
[1,2]Assistant Professors in Computer Science
[3]Associate Professor in Computer Science
Gobi Arts & Science College (Autonomous)
Gobichettipalayam, T.N India
ramsgobi@gmail.com, drprabhusundhar@gmail.com

Abstract—In wireless mobile ad hoc network, mainly, two approaches are followed to protect the security such as prevention-based approaches and detection-based approaches. A Mobile Ad hoc Network (MANET) is a collection of autonomous wireless mobile nodes forming temporary network to interchange data (data packets) without using any fixed topology or centralized administration. In this dynamic network, each node changes its geographical position and acts as a router for forwarding packets to the other node. Current MANETs are basically vulnerable to different types of attacks. The multimodal biometric technology gives possible resolves for continuous user authentication and vulnerability in high security mobile ad hoc networks (MANETs). Dempster's rule for combination gives a numerical method for combining multiple pieces of data from unreliable observers. This paper studies biometric authentication and intrusion detection system with data fusion using Dempster–Shafer theory in such MANETs. Multimodal biometric technologies are arrayed to work with intrusion detection to improve the limitations of unimodal biometric technique.

Keywords- *Mobile Ad hoc network, Dempster–Shafer theory, Intrusion Detection System.*

*****

I. INTRODUCTION

This paper is concerned with the study and analysis of biometric-based security for mobile ad hoc network to progress the security in order to decrease the network attacks and leakage of information. With the propagation of inexpensive, smaller and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the wildest growing areas of research and it becomes a popular research subject due to their self-configuration and self-maintenance capabilities. Wireless nodes can initiate a dynamic network without a static infrastructure. This type of network is very useful in tactical operations where there is no communication setup. However, security is a major concern for providing reliable communications in a potentially hostile situation. This new type of self-organizing network combines wireless communication with a high degree node mobility. Unlike, conventional wired networks mobile ad hoc networks don't have fixed structure (base stations, centralized management points and the like). The union of nodes forms an arbitrary topology. This malleable nature makes them attractive for many applications such as military applications, where the network topology may change rapidly to reflect a force's operational movements and disaster recovery operations, where the existing/fixed infrastructure may be non-operational. The ad hoc self-organization also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming high-cost task. Basic functions like packet forwarding, routing and network management are accomplished by the dedicated nodes in the conventional networks. In ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication: nodes within the radio range can communicate directly via wireless links, meanwhile nodes which are far must rely on intermediate nodes to act as routers to relay messages. Mobile nodes can move, leave and join the network and routes are need to be updated frequently due to the dynamic network topology.

II. MANET SECURITY

Because of MANET's special characteristics, there are some important metrics in MANET security that are important in all security approaches; call them "Security Parameters". Being unaware of these parameters may cause a security approach useless in MANET. Figure 1. shows the relation between security parameters and security challenges. Each security approach must be aware of security parameters as shown in Figure 1. All mechanisms proposed for security aspects, must be aware of these parameters otherwise they may be useless in MANET. Security parameters in MANET are as follows:

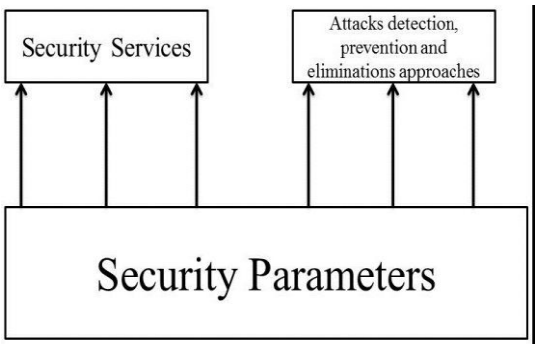

Figure 1. Relation between Security Parameters and Security aspects [Ali Dorri et al., 2015]

Network Overhead: This parameter refers a number of control packets generated by security approaches. Due to shared wireless media, additional control packets may easily congestion or collision in MANET. Packet lost is one the results of congestion and collision. Therefore, high packet overhead increases packet lost and the number of retransmitted packets. This process could easily waste nodes energy and networks resources.

Processing Time: Each security approach needs time to detect misbehaviors and eliminate malicious nodes. Due to MANET's dynamic topology it's strongly possible that routes between two different nodes break because of mobility. Therefore, security approaches must have as low as possible processing time in order to increase MANET flexibility and avoid rerouting process.

Energy Consumption: In MANET nodes have limited energy supply. Therefore, optimizing energy consumption is highly challengeable in MANET. High energy consumption reduces nodes and network's lifetime. Each security protocol must be aware of these three important parameters. In some situations, a trade-off between these parameters is provided in order to perform a satisfaction level in all of them. Security protocols that disregard these parameters aren't efficient as they waste network resources [Ali Dorri et al., 2015].

III. MANET SECURITY CHALLENGES

Generally, there are two important aspects in security: Security services and Attacks. Services refer to some protecting policies in order to make a secure network, while attacks use network vulnerabilities to defeat a security service. **Security Services** The aim of a security service is to secure network before any attack has happened and made it harder for a malicious node to break the security of the network. Due to special features of MANET, providing these services face lot of challenges. For securing MANET, a trade-off between these services must be provided, means that, if one service guarantees without the notice of other services, security system will fail. Providing a trade-off between these security services depend on the network application, but the problem is to provide services one by one in MANET and presenting a way to guarantee each service. The below section discuss five important security services and their challenges as follows:

Availability: According to this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and open boundary. Accessing time is the time needed for a node to access the network services or data. It is important, because time is one of the security parameters. Authors provided a new way to solve this problem by using a new trust based clustering approach. In the proposed approach which is called ABTMC (Availability Based Trust Model of Clusters), by using availability based trust model, hostile nodes are identified quickly and should be isolated from the network in a period of time, therefore availability of MANET will be guaranteed.

Authentication: The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, whoever, in absence of central control unit, key distribution and key management makes challengeable. Ali Dorri et al., [2015] presented a new way based on trust model and clustering to public the certificate keys. In this case, the network is divided into some clusters and in this clusters public key distribution will be safe [Ali Dorri et al., 2015]. But it has some limitations like clustering. MANET dynamic topology and unpredictable nodes position, made clustering challengeable.

Data confidentially: According to this service, each node or application must have access to specified services that are permitted to access. Most of the services that are provided by data confidentially use encryption methods, but in MANET, as there is no central management, key distribution faces lots of challenges and in some cases impossible. Authors proposed a new scheme for reliable data delivery to enhance the data confidentially. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination. Therefore, even if a small number of nodes that are used to relay the message shares, been compromised, the secret message as a whole is not compromised. Using multipath delivering causes the variation of delay in packet delivery of different packets. It also leads out-of-order packet delivery.

Integrity: According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them. Authors presented a mechanism to modify the DSR routing protocol and gain data integrity by securing the discovering phase of routing protocol.

Non-Repudiation: By using this service, neither source nor destination can repudiate their behavior or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent. Authors presented a new approach that is based on grouping and limiting hops in broadcast packets. All group members have a private key to ensure that another node couldn't create packets with its properties. But creating groups in MANET is challengeable [Ali Dorri et al., 2015].

IV. BIOMETRIC SECURITY

A *biometric* is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics are known as the science of *biometrics*. In those days, biometric technologies are typically used to analyze human characteristics for security purposes. The most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face and voice [Colin Soutar et al., 1999].

A. Biometric-Based User Authentication

Biometric technology can be used automatically and continuously identify or verify individuals by their physiological or behavioral characteristics. Biometric systems include two kinds of operation models: 1) identification and 2) authentication. In the proposed system, the biometric systems operate in authentication mode, (one-to-one match process) to address a common security concern: positive verification (the user is whoever the user claims to be). In most real-world implementations of biometric systems, biometric templates are stored in a location remote to the biometric sensors. In biometric authentication processes, two kinds of errors can be made: 1) false acceptance (FA) and 2) false rejection (FR). FAs result in security breaches since unauthorized persons are admitted to access the system/network. FRs result in convenience problems since genuinely enrolled identities are denied access to the system/network and maybe some further checks need to be done. The frequency of FA errors and of FR errors is called FA rate (FAR) and FR rate (FRR), respectively. The FAR can be used to measure the security characteristics of the biometric systems since a low FAR implies a low possibility that an intruder is allowed to access the system/network. In tactical MANETs, failure in user authentication might result in serious consequences. Hence, more than one biometric sensor is used at each time period in the system to increase the effectiveness of user authentication [K.K.Lakshmi Narayanan et al., 2012]. The classification of biometrics shown in figure 2.

B. Multimodal Biometric Systems

In order to overcome the disadvantages of uni-modal biometrics, biometrics to be ultra-secure and to provide more-than-average accuracy, more than one form of biometrics is required and hence, the need arises for the use of multimodal biometrics. Instead of using a single biometrics, a combination of different biometric can be used for recognizing a human being. Multimodal biometric can be composed in three different fusion methodologies, such as fusion at the feature level, match score level and decision level. As fourth level, a new fusion technique is used in this work, which fuses the security services provided by the system by adding more biometric modalities the security level increases. [Snehlata Barde et al., 2012].

C. Operational modes of multimodal biometric systems

It is evident that a single biometric trait is not enough to meet the variety of requirements including matching performance and recognition accuracy imposed by several large-scale authentication systems. Multimodal biometric recognition systems appear more reliable due to the presence of multiple, independent pieces of data. A multimodal biometric system can operate in three different modes. In the ***serial mode*** of operation, the output of one biometric trait is used to narrow down the number of possible identities before the next trait is used. In a ***parallel mode*** of operation, information from multiple traits is used simultaneously to perform recognition. In the ***hierarchical scheme***, individual classifiers are combined in a treelike structure.

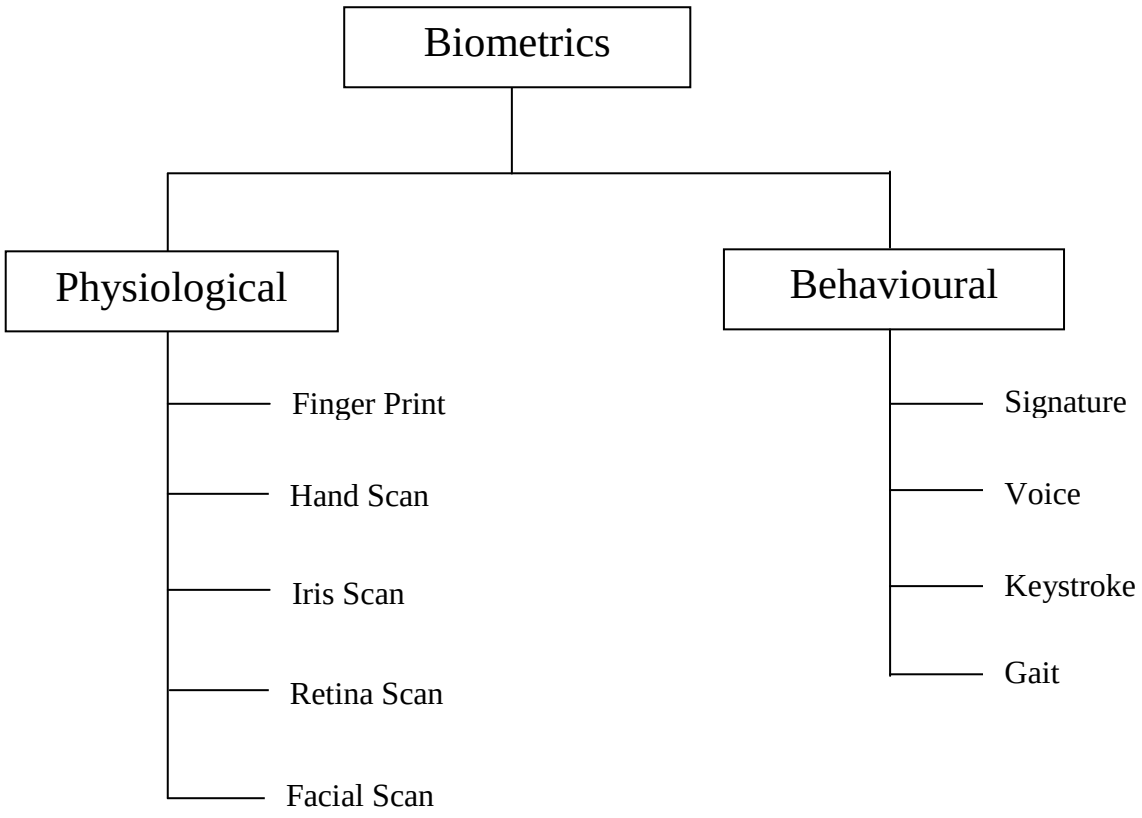

Figure 2. Two Biometric Families [Claude Barral 2010]

V. INTRUSION DETECTION SYSTEM

Intrusion detection is a process of monitoring computer networks and systems for violations of security and can be automatically performed by IDS. User authentication is performed by using one or more types of validation factors: knowledge factors, possession factors, and biometric factors. Knowledge factors (such as passwords) and possession factors (such as tokens) are very easy to implement but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. Biometrics technology, such as the recognition of fingerprints, irises, faces, retinas, etc., provides possible solutions to the authentication problem. Using this technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption. In addition, intrusion detection systems (IDSs) are important in MANETs to effectively identify malicious activities and so, MANET may appropriately respond. IDSs can be categorized as follows: 1) network-based intrusion detection, which runs at the gateway of a network and examines all incoming packets; 2) router-based intrusion detection, which is installed on the routers to prevent intruders from entering the network; and 3) host-based intrusion detection, which receives the necessary audit data from the host's operating system and analyzes the generated events to keep the local node secure. For MANETs, host-based IDSs are suitable, since no centralized gateway or router exists in the network.

Two main technologies of identifying intrusion detection in IDSs are given as follows: misuse detection and anomaly detection. Misuse detection is the most common signature-based technique, where incoming/outgoing traffic is compared against the possible attack signatures/patterns stored in a database. If the system matches the data with an attack pattern, the IDS regards it as an attack and then raises an alarm. Unable to detect new forms of attack is the main drawback of misuse detection. Anomaly detection is a behavior-based method, which uses statistical analysis to find changes in baseline behavior. This technology is weaker than misuse detection but has the benefit of catching the attacks without signature existence. Multiple algorithms have applied in model attack signatures or normal behavior patterns of systems. Three common algorithms are naive Bayes, artificial neural network (ANN) and decision tree (DT). A naive Bayes classifier is based on a probabilistic model to assign the most likely class to a given instance. ANN is a pattern recognition technique with the capacity to adaptively model user or system behavior. DT, which is a useful machine learning technique, is used to organize the attack signatures to a tree structure. Most of the IDSs only use one of the preceding algorithms [K.K.Lakshmi Narayanan and A.Fidal Castro, 2012].

IDS Protocol

The IDS protocol is classified as, *region-voting-based IDS* and *group voting based IDS*. Both protocols derive the concept of distributed revocation based on majority voting for evicting a target node in the context of sensor networks. To do so, each node is preinstalled with *host-based* IDS to collect information to detect the status of neighboring nodes. Techniques such as misuse detection (also called signature based detection) and anomaly detection can be used to implement host-based IDS in each node. The effectiveness of host-based IDS is measured by two parameters, namely, the *per-node* false negative probability (*p1*) and *per-node* false positive probability (*p2*). In voting-based IDS, compromised nodes are detected based on majority voting. If the majority decide to vote against the target node, then the target node would be evicted from the system. This adds intrusion tolerance to tolerate collusion of compromised nodes in MANETs. Jin-Hee Cho and Ing-Ray Chen [2008] explained and characterized voting-based IDS by two parameters, namely, false negative probability (*Pfn*) and false positive probability (*Pfp*). These two parameters are calculated based on (a) the *per-node* false negative and positive probabilities (*p1* and *p2*); (b) the number of vote-participants, *m*, selected to vote for or against a target node; and (c) an estimate of the current number of compromised nodes which may collude with the objective to disrupt the service of the system. Since *m* nodes are selected to vote, if the majority of *m* voting-participants casts negative votes against a target node, the target node is considered compromised and will be evicted from the system. The two voting-based algorithms investigated in [Jin-Hee Cho and Ing-Ray Chen, 2008], namely, *region-voting-based IDS* and *group-voting-based IDS*, are differentiated by the way *m* vote-participants are selected when evaluating a target node. Each node periodically exchanges its routing information, location, and *id* to its neighboring nodes. In *region-voting-based IDS*, only nodes in the same geographical "region" are candidates as vote-participants with respect to a target node. [Jin-Hee Cho and Ing-Ray Chen, 2008].

VI. DEMPSTER-SHAFER THEORY

The Dempster-Shafer evidence theory is not only a theory of evidence but also a probable reasoning. It is a framework that can be deployed in diverse areas such as pattern matching, computer vision, expert systems and information retrieval. The D-S evidence theory can handle the randomness and subjective uncertainty together in the trust evaluation. By accumulating evidences, it can narrow down a hypothesis set which provides a powerful method for the representation and process of the trust uncertainty without the demand of prior distribution. Moreover, Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidence [Bo YANG et al., 2013].

Without a fixed security infrastructure, mobile ad hoc networks must distribute intrusion detection among their nodes. But even though a distributed intrusion detection system can combine data from multiple nodes to estimate the likelihood of an intrusion, the observing nodes might not be reliable. The Dempster-Shafer theory of evidence is well suited for this type of problem because it reflects uncertainty. Moreover, Dempster's rule for combination gives a numerical procedure for fusing together multiple pieces of evidence from unreliable observers [Thomas M, 2005].

The Dempster-Shafer (DS) theory for uncertainty was first developed by Arthur Dempster [P. Dempster,1968] and extended by Glenn Shafer [G. Shafer,1976]. The theory provides necessary tools for combining various evidences and gives them various weightings, according to their importance in the final decision making, their quality and relevance. Glenn Shafer et al., justify the use of the DS theory by the uncertain nature of the trust prediction problem and the need to combine the different criteria (evidences) and concerned with the value of some quantity u, and the set of its possible values is U. The set U is called frame of discernment. In the prediction scheme, the frame of discernment U is a trust value of mobile node which is able to become the trusted nodes in future. The frame of discernment is U {T, ØT}, m(A) represents the exact belief committed to A, according to the evidence associated with each node's opinion about the Suspicious node. If m(A) > 0 then A is called a focal element. The focal elements and the associated bpa define a body of evidence. Each subset of U is assigned a probability that represents the belief affected by the evidence. This confidence value is usually computed based on a density function m: 2U → [0, 1] called a basic probability assignment (bpa) function.

$$m(\phi) = 0, \sum A \subseteq U m(A) = 1$$

CH has got the information from neighbor nodes and the following probability assignments are given. If received trust value t>0.5, the node is treated as trusted. If received trust value t<0.5, node is treated as untrusted and the probability is assigned accordingly.

m1 ({T}) = 0.8

m1 ({¬ T}) = 0

m1 ({T, ¬ T}) = 0.2 [This state is for Suspicious]

And the CH has the probability assignments on the same node

m2 ({T}) = 0.6

m2 ({¬ T}) = 0

m2 ({T, ¬ T}) = 0.4 [This state is for Suspicious]

A. The Dempster Combination Rule

Let m1 and m2 be the bpa associated with two independent bodies of evidence defined in a frame of discernment U. The new body of evidence is defined by a bpa, m on the same frame U.

$$K = \sum_{B \cap C = \phi} m1(B)m2(c)$$

$$m(A) = m1 \otimes m2 = K^{-1} \sum_{B \cap C = A} m1(B)m2(C)$$

The rule focuses only on those propositions that both bodies of evidence support. The K of the above equation is a normalization factor that ensures that m is a bpa. The combination rule is commutative and associative. In this approach, the clusterhead computes the trust of each node according to each criterion (evidence) and combines them two by two. An example solution is illustrated in Table 1. Therefore,

m1 $\otimes$ m2 ({T}) = (1) (0.24+0.32+0.12) = 0.68

m1 $\otimes$ m2 ({$\neg$T}) = (1) (0) = 0

m1 $\otimes$ m2 ({T, $\neg$T}) = (1) (0.08) = 0.08

	m2			
m1		{T}:0.6	{$\neg$T}:0	{T, $\neg$T}:0.4
	{T}: 0.8	.24	0	.32
	{$\neg$T}: 0	0	0	0
	{T, $\neg$T}: 0.2	.12	0	.08

Table 1. An example of combining evidences using DS Theory [Pushpita Chatterjee, 2009]

So the given evidence presented here by m1 and m2, the most probable belief for this Universe of discourse is T with probability 0.68. Any CH will execute this algorithm for getting the most probable belief after collecting recommendation trust from others [Pushpita Chatterjee, 2009].

B. Design of Multimodal Biometric IDS System

Biometric-Based User Authentication: Biometric technology can be used to automatically and continuously recognize two types of operation models: (i) identification and (ii) authentication.

Step 1: select sensor u_{k+1} that will be used at time k+1

Step 2: at time k+1, observe the output of sensor u_{k+1}

{Observation $y_k+1=y_k+1(u_{k+1})$}

Step 3: update information state π_{k+1} with observation y_{k+1}

Figure 3. Sensor scheduling and information state update

In the proposed model, the biometric systems operate in authentication mode to address a common security concern: positive verification based on a comparison of the matching score between the input sample and the enrolled template with a decision threshold. Improved intrusion detection model: Intrusion detection is a process of observing computer networks and systems for abuses of security. Two key technologies of detecting intrusion detection in IDS are given as follows: (i) misuse detection and (ii) anomaly detection [Jie Liu et al., 2009].

Step 1: Biometric technology can be used automatically and continuously identify the physiological or behavioral characteristics

Step 2: Biometric-Based User Authentication: two kinds of operation models: i) identification and ii) authentication

Step 3: Sensors are chosen for continuous authentication and IDS at each time space to detect the security formal of the network

Step 4: Dempster–Shafer reasoning system: Set of mutually exclusive and exhaustive possibilities is enumerated in the frame of discernment and two security states for each node: secure and compromised state

Step 5: Fusion of biometric sensors and IDS

Figure 4. Biometric based IDS Procedure

Data fusion of biometric sensors: In the proposed model, sensors are picked for authentication and intrusion detection at each time slot to detect the security state of the network. Two major fusions are used to select the biosensor such as class set reduction (CSR) and a class set reordering (CSRR). CSR methods try to find the minimal reduced class set, in which the true class is still represented. CSRR methods try to increase the true class ranking as high as possible. It produces soft outputs, which are the real values in the range [0, 1]. Dempster–Shafer theory: In a Dempster–

Shafer reasoning system, a set of mutually exclusive and exhaustive possibilities is enumerated in the frame of discernment. In this two security states for each node, secure and compromised states are used in the Dempster–Shafer theory in the fusion of biometric sensors and IDS.

VII. CONCLUSION

In this research exposition, the MANET security systems have been studied and classified into prevention-based approaches such as authentication and detection-based approaches such intrusion detection. The biometric method improves the network security, in order to achieve high security and good reliability in ad hoc network even the high number of nodes. Further, analysis the existing multimodal biometric based IDS system, operational modes of multimodal biometric systems, data fusion, IDS protocol and Dempster combination Rule.

References:

[1] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah, 2015., *"Security Challenges in Mobile Ad Hoc Networks: A Survey"*, International Journal of Computer Science & Engineering Survey (IJCSES), Vol. 6, No. 1, pp. 15 – 29, February 2015.

[2] Arnab Maji., 2010., *"Load Balancing in Wireless Mobile Ad hoc Networks"*, Bachelor of Technology, National Institute of Technology, Rourkela.

[3] Ali Hilal Al-Bayatti., 2009., *"Security Management for Mobile Ad hoc Network of Networks (MANoN)"*, De Montfort University.

[4] Bo Yang, Ryo Yamamoto and Yoshiaki Tanaka., 2013., *"Dempster-Shafer Evidence Theory Based Trust Management Strategy against Cooperative Black Hole Attacks and Gray Hole Attacks in MANETs"*, ICACT Transactions on Advanced Communications Technology(TACT), Vol. 2(3), pp. 223 – 232, May, 2013.

[5] Claude BARRAL., 2010., *"Biometrics & Security:Combining Fingerprints, Smart Cards and Cryptography"*, in the proceedings of ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE.

[6] Carvallo M., and Garcia Luna Aceves J.J., 2004., *"A Scalable Model for Channel Access Protocols in Multihop Ad Hoc Networks"*, IEEE Conference on Mobile Computing and Networking, pp. 330 – 344.

[7] Dempster P., 1968., "*A Generalization of Bayesian Interface*", Journal of Royal Statistical Society, pp. 205 – 447.

[8] Jie Liu, Richard Yu F, Chung-Horng Lung and Helen Tang., 2008., *"A Framework of Combining Intrusion Detection and Continuous Authentication in Mobile Ad Hoc Networks"*, in the proceedings of ICC 2008 of IEEE Communications Society, 978-1-4244-2075-9/08/$25.00 ©2008 IEEE, pp. 1515 – 1519.

[9] Jain A.K., Ross A. and Prabhakar S., 2004., *"An Introduction to Biometric Recognition"*, in the proceedings of IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, pp. 4 – 20, Jan, 2004.

[10] Jain A.K., Bolle R. and Pankanti S., 1998., *"Biometrics, PersonalIdentification in Networked Society: Personal Identification in Networked Society"*, Kluwer Academic Publishers, Norwell, MA, USA.

[11] Jin-Hee Cho and Ing-Ray Chen., 2008., *"Effect of Intrusion Detection on Secure Group Communications in Hierarchically Structured Group Architectures"*, in the proceedings of IEEE Transactions, pp. 942 – 949.

[12] 12. Lakshmi Narayanan K K, Fidal Castro A., 2012., *"High Security for Manet Using Authentication and Intrusion Detection with Data Fusion"*, International Journal of Scientific & Engineering Research, Vol. 3, Issue 3, pp. 1 – 4, March, 2012.

[13] Luc Hogie., 2007., *"Mobile Ad Hoc Networks: Modelling, Simulation and Broadcast-Based Applications"*, University of Le Havre, University of Luxembourg.

[14] Marco Conti, Silvia Giordano, Gaia Maselli, and Giovanni Turi., 2004., *"Mobile Metropolitan Ad hoc Networks"*, in the proceedings of the 8th International IFIP-TC6 Conference, Lecture Notes in Computer Science, LNCS - 2775, pp. 194 – 205.

[15] Macker J.P., and Corson S., 2003., *"Mobile Ad hoc Networks (MANET): Routing Technology for Dynamic, Wireless Networking in Mobile Ad hoc Networking"*, IEEE, Press and John Wiley and Sons, Inc., New York.

[16] Pushpita Chatterjee., 2009., *"Trust Based Clustering and Secure Routing Scheme for Mobile Ad Hoc Networks"*, International Journal of Computer Networks & Communications (IJCNC), Vol. 1, No. 2, pp. 84 – 97, July, 2009.

[17] Prabhusundhar P, Dr. Srinivasan B and Narendirakumar V K., 2013., "*Border Crossing Security and Privacy in Biometric Passport using Cryptographic Authentication Protocol*", in the proceedings of International Conference on Computer Communication and Informatics (ICCCI), 4th to 6th January 2013, IEEE Catalog Number: CFP1308R-CDR (CD), ISBN 978-1-4673-2905-7 ©2013 IEEE, pp. 1 – 7.

[18] Prabhusundhar P and Dr. Srinivasan B., "*Identification of Biometric- Based Continuous User Authentication and Intrusion Detection System for Cluster Based MANET*", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN No. 2321-8169 (print), Vol. 4, No. 3, March- 2016, pp. 207 – 213.

[19] Prabhusundhar P and Dr. Srinivasan B., "*Multimodal Biometric Based Intrusion Detection System for Clustered Mobile Ad Hoc Network*

Using POMDP Algorithm", KASMERA Journal (Science Citation Indexed Journal), ISSN: 0075-5222, Vol. 44, No. 1, pp. 2 – 9.

[20] Raghu Trivedi T. and Dr. Seshadri R.., *"Efficient Cryptographic Key Generation using Biometrics"*, International Journal of Comp. Tech., Vol. 2, No. 1, pp. 183 – 187.

[21] Ramalingam M and Dr. Thiagarasu V., *"Cluster Based Stretch and Shrink Method for Manet Using Load Balancing, Nearest Neighbor and Rule Mining"*, International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, P.no 392-400, Oct-2014.

[22] Ramalingam M and Dr. Thiagarasu V., *"Identified the Cluster Based Stretch and Shrink Method Based On Load Balancing Algorithm for Ad Hoc Network Topology Stability*", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 2 Issue: 9 p.no: 2631 – 2635

[23] M. Ramalingam, Dr.V Thiagarasu, "Routing and Broadcasting in MANET: A comprehensive Analysis based on, Routing technique, Clustering and Architectural Model", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, IJESRT 3 (11),November 2014.

[24] Shengrong Bu, Richard Yu F, Xiaoping P. Liu, Peter Mason and Helen Tang., 2011., *"Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks"*, IEEE Transactions On Vehicular Technology, Vol. 60, No. 3, March 2011, Pp. 1025 – 1036.

[25] Shafer G 1976., "*A Mathematical Theory of Evidence*", Princeton University Press.

[26] Thomas M. Chen and Varadharajan Venkataramanan., 2005., *"Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks"*, in the proceedings of IEEE INTERNET COMPUTING, Published by the IEEE Computer Society, pp. 35 – 41.