International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 3 207 -213

Identification of Biometric-Based Continuous user Authentication and Intrusion Detection System for Cluster Based Manet

[1]P. Prabhusundhar, [2]Dr. B. Srinivasan
[1] Assistant Professor, Department of Information Technology,
[2] Associate Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
Email ID: [1] prabhusundhar@yahoo.co.in , [2] srinivasan_gasc@yahoo.com

Abstract-Mobile ad hoc is an infrastructure less dynamic network used in many applications; it has been targets of various attacks and makes security problems. This work aims to provide an enhanced level of security by using the prevention based and detection based approaches such as authentication and intrusion detection. The multi-model biometric technology is used for continuous authentication and intrusion detection in high security cluster based MANET. In this paper, an attempt has been made to combine continuous authentication and intrusion detection. In this proposed scheme, Dempster-Shafer theory is used for data fusion because more than one device needs to be chosen and their observation can be used to increase observation accuracy.

Keyword- *MANET; WCA; Biometrics; Intrusion Detection; Security.*

*****

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a collection of autonomous wireless nodes that communicate dynamically and establishes the network to exchange the information. Ad hoc Network can be created and used at anytime, anywhere without using any fixed topology or centralized administration. The ability of self-configuration of MANET can be used in conferences, meetings, natural disasters, crowd controls, battle fields and emergency situations [14]**.** MANET is unlike fixed hardwired networks with physical defence at firewalls and gateways, attacks on ad hoc networks can come from all directions and may target any node. Autonomous nodes have inadequate physical protection and can be captured, compromised, and hijacked easily. Attacks from a compromised node are more dangerous and much harder to detect. Damage includes leaking secret information, interfering message and impersonating nodes, thus violating the basic security requirements. All these mean that every nodes must be prepared to encounter with an adversary directly or indirectly [21]. User authentication and preventing unauthorized users from accessing resources are difficult in MANET. Due to these reasons MANET is particularly vulnerable to various types of attacks such as inside attack, outside attack *active and passive attacks*. Various security mechanisms have been proposed in ad hoc network such as password, possession factors, and biometrics. The Biometric techniques are playing an important role in authentication such as the recognition of faces ,fingerprints, irises, retinas, etc and by using this technique user can continuously identified by their physiological characteristics [1].

Malicious activities by misbehaviour node can be efficiently identified by intrusion detection systems (IDSs). IDSs can be classified in to three types [3]: (i) Gate way nodes have network-based intrusion detection: used to inspecting all incoming packets, so this can be implemented in gateway nodes. (ii) Router nodes have router-based intrusion detection: used to protect intruders in MANET (iii) Host-based intrusion detection: used to protect the local node by using audit information from its neighbour. Rather, a cooperative approach is required, involving collaboration and exchange of observations by larger collections of nodes. Hierarchical IDS architectures organize cooperative intrusion detection activities into a multi-level intrusion detection hierarchy, in which each node gathers network traffic data and reports these to its parent [28] [16]. Hierarchical IDS architecture is developed for mobile ad hoc multi-layered networks. In a multilayered structure, head nodes (CH-Cluster Head) are responsible for centralized routing in cluster group and may support additional security mechanisms [2].

The Dempster-Shafer (DS) theory has developed by Arthur Dempster and extended by Glenn Shafer. The DS theory provides essential tools to merge a choice of evidences and gives them various weightings, based on the importance in the final decision making its quality and relevance. Pushpita C, [2013] justified the use of the DS theory by the uncertain nature of the trust prediction problem and the need to combine the different criteria (evidences) [21]. Bo Yang et al., [2013] explained the Dempster-Shafer evidence theory is a framework that can be implemented in diverse areas such as computer vision, pattern matching, expert model and information retrieval. It is not only a theory of evidence but also that of probable reasoning. This theory can maintain the randomness and subjective uncertainty together in the trust evaluation. By gathering 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 and in this paper the whole system as a partially observed Markov decision process considering both system security requirements and resource constraints [15].

II. CLASSIFICATIONS OF SECURITY ATTACKS IN MANET

A Security Mechanism is a process in MANET and the most important concern for the basic functionality of network. A Security Service can be recognized as a processing service expected to increase the security of data. MANET frequently affects from security attacks because of its unique characteristic such as open medium, dynamic topology, infrastructure less and lack of central monitoring and management[16]. MANETs security attacks can be classified into three different ways like i. Inside and Outside Attacks ii. Active and passive attacks are shown in table1 and iii. Classification Based on Layers [18].

A. Inside and Outside Attacks

This type of attack mostly aimed on mobile nodes available in the boundary of ad hoc network. It is most hazardous attack as malicious node can do much harm to other nodes and also affecting the routing data process happening in the mobile ad hoc environment. Different kinds of attacks are sinkhole attack, routing attacks, Dropping Attacks and eavesdropping. The MANET routing nodes are attacked by the outside attacks staged by a node. These attacks can be organized in different ways like DoS, impersonation and outside attacks are measured less effective as compared to inside attacks. Mohammed .M, [2014] [18] analyzed and classified of insider attacks into atomic misuses (in which a single routing message is manipulated) and compound misuses (in which a combination of atomic misuses is employed). The study showed several classes of insider attacks, including route disruption, route invasion, node isolation, and resource consumption.

Sinkhole Attack: In a *blackhole* attack, or sometimes referred to as sinkhole attack, the exploited node advertises routes to other nodes passing through itself, and when other nodes start passing packets to the exploited node to forward them, the node drops the packets and does not forward anything out [23].

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. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.

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 Behaviour 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 neighbouring nodes. Many routing techniques in MANETs assume good faith when it comes to trusting other nodes in the network. This assumption does not always hold [18].

B. Active and Passive Attacks

The MANET network operation can be disturbed by the active attack and it can distress the MANET process in different ways such as affecting data routing and routing node, battery draining and stopping packets delivery to the destination node or rendering service unusable. Both type of nodes like inside and outside nodes are attacking the network and it is using the following methods to affecting the network operation: spoofing and escalate are more dangerous forms like DoS, modification of messages, sinkholes, and Sybil attacks. Instead of interrupt the flow of data packed, the passive attacks collecting information about the network. Eavesdropping, monitoring, and traffic analysis are listed in the passive attack.

C. Classification Based on Layers

Attacks on MANETs can also be classified based on the Open Systems Interconnection (OSI) layered model. Table 2 shows the classification of attacks based on the layer they operate at.

Table 1: Active and Passive Attacks [4]

Active Attacks	Spoofing
	Fabrication
	Wormhole Attack
	Modification
	Denial of Service
	Denial of Service
	Blackholes and Grayholes
	Sybil Attack
Passive Attacks	Eavesdropping
	Monitoring
	Traffic Analysis

Table 2: Attacks Classified Based On OSI Layers [5][18]

Layer Attack(s)	**Layer Attack(s)**
Multi-Layer	DoS, impersonation, replay, man-in-the-middle
Application	Repudiation, data corruption
Transport	Session hijacking, SYN flooding
Network	Wormhole, blackhole, greyhole, Byzantine, flooding, resource consumption, location disclosure attacks, routing table overflow
Data Link	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical	Jamming, interceptions, eavesdropping

III. INTRUSION DETECTION SYSTEM

Intrusion detection system (IDS) [6] is responsible for collecting audit data and reasoning about the verification in the data to decide the system in attack. Mainly the IDS can be classified into two types such as network based and host based. A network based IDS normally runs at the gateway node and collect the network packets in MANET and host based system individual IDS are placed on each and every node to monitors local activities [17]. R.M.Chamundeeswari et al., [2015] classified the IDS in the following two methods to detecting the intrusion such as misuse based intrusion detection (also called knowledge-based detection) and anomaly based intrusion detection (also called as behaviour-based).The Misuse intrusion detection refers to the detection of intrusions which are accurately crucial and further on time by watching for the incidence. There is a misuse constituent in the majority intrusion detection systems as statistical techniques unaided are not sufficient to detect all types of intrusions. Since statistical techniques alone are not adequate to detect all types of intrusions. Anomaly detection is the detection of items, actions or annotations which do not be conventional to a predictable pattern or other items in a dataset. Typically the irregular items determination decode to some variety of difficulty such as bank fraud, a structural defect, check up problems or finding errors in content. It stands against anomaly detection technique which utilizes the reverse technique of misuse intrusion detection. The anomaly detection is take first step to defining usual system behaviour and then defining at all other behaviour as irregular. Intrusion detection techniques can be classified into many ways i) Active Intrusion Detection ii) Passive Intrusion Detection iii) Network Intrusion Detection iv) Host Intrusion Detection

An **Active Intrusion detection** system is as well described as Intrusion Detection and Prevention System. This system is configured to repeatedly block supposed attacks devoid of any interference required by an operator. This system has the gain of offering real time remedial action in response to an attack. The **Passive Intrusion detection** is a system to facilitate configured to only monitor and evaluate network traffic activity and alerts an operator to probable vulnerabilities and attacks. A passive intrusion detection system is not competent of performing any defensive or remedial functions on its own. The **Network Intrusion Detection** Systems frequently consists of a network sensor with a Network Interface Card operating in dissolute mode and a divide management interface. The intrusion detection system is located beside a network sector or boundary and monitors all traffic on those sectors. The **Host Intrusion Detection** Systems and software relevance mediator installed on workstations which are to be monitored. The mediator monitors the operating system and writes data to log records and activate alarms. A host Intrusion detection systems can only observes the creature workstations on which the mediators are installed and it cannot supervise the total network. Host based IDS systems are used to observe any intrusion attempts on grave servers [12].

Hierarchical IDS Architecture and LS-WCA Clusterhead Selection

Azin Moradmand B et al., 2013 explained hierarchical IDS architectures organize cooperative intrusion detection activities into a multi-level intrusion detection hierarchy, in which each node gathers network traffic data and reports these to its parent. The hierarchical IDS architecture proposes splitting the nodes of a MANET into clusters with cluster-heads. Cluster-heads act as a tiny base station for the nodes within its cluster and aggregate information about malicious activities from those member nodes. Cluster-heads in turn cooperate with a central station (the root) to form IDS global to the MANET. The imposition of this hierarchical structure on the MANET is designed firstly to overcome the lack of central administration in MANETs, secondly to form a tree-based structure robust in the face of network changes and that enables the rapid aggregation of detection data, and thirdly to acquire enough aggregated network traffic data, from vantage points throughout the MANET, to reach accurate decisions about attacks [13].

Load Sharing in Weighted Clustering Algorithm (LS-WCA) has been developed by Ratish Agarwal et al., [2014] [10].

Degree Difference: In cluster-based structure a performance parameter for load balancing is *degree difference* (Δ_v), for each node *v* which is defined as the difference of ideal node degree (δ) and actual degree (connectivity) of that node. Degree of node (d_v) is the number of neighbours of node *v* that are in the transmission range. Ideal degree is the number of neighbours that a clusterhead can handle effectively.

$$Degree\ difference\ (\Delta_v) = |d_v - \delta|$$

Energy Consumption: Clusterhead has to perform extra task for routing and forwarding the packets, so it is more prone to energy drainage.

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2 \text{ Or}$$

$$P_t \propto R^2$$

where, P_t is transmitted power and P_r is power at the receiving antenna, G_t and G_r are the antenna gains, λ is the wavelength used and *R* is the distance between the nodes. Energy-consumption of a node is directly proportional to the distance of that node with its neighbours.

Sum of distance to all neighbours (S_{dv}) is found as

$$Sd_v = \frac{1}{dv} \sum_k \sqrt{(x_v - x_k)^2 + (y_v - y_k)^2}$$

Where (x_v, y_v) and (x_k, y_k) are the coordinates of the node *v* and node *k* respectively. Summation is donefor all neighbours *k* of node *v*.

Mobility: Mobility or stability is an important factor in deciding the clusterheads. In order to avoid frequent clusterhead changes, it is desirable to elect a clusterhead that does not move very quickly. When the clusterhead moves fast, the nodes may be detached from the clusterhead and as a result, a re-affiliation occurs. Re-affiliation is not a desirable feature because it can increase computation and processing. The running average of the speed for every node till current time *T* gives a measure of mobility and is denoted by M_v, as

$$M_v = 1/T \sum_{t=1}^{T} \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2}$$

Where (x_t, y_t) and ($x_t - 1$, $y_t - 1$) are the coordinates of the node *v* at time *t* and ($t - 1$) respectively.

Power: A clusterhead consumes more battery than an ordinary node because it has extra responsibilities. It can estimate the remaining battery power by the amount of time spent by the node as a clusterhead. The parameter P_v is the cumulative time of a node being a clusterhead. P_v is used to measure how much battery power has been consume by the node. Higher the value of P_v lower the remaining battery power. All four parameters (Δ_v, Sd_v, M_v , and P_v,) explained above can be used as a performance matrix for selection of a node as a clusterhead. Weight of these parameters can change according to requirement. Combined weight of a node W_v is calculated as follows

$$W_v = W_1.\ \Delta_v + W_2.Sd_v + W_3.M_v + W_4.P_v$$

Each node calculates its weight and broadcasts it periodically in a hello packet to all nodes in its transmission range. When a node receives the weights of its 1-hop neighbours, it inserts them in the possible CH set, which includes all potential cluster-heads.

IV. BIOMETRIC-BASED CONTINUOUS USER AUTHENTICATION AND INTRUSION DETECTION IN MANET

The biometric methods are used to automatically and continuously identifying unique human characteristics as a mean of authenticating or verify individuals by their physiological or behavioural characteristics. Biometric systems include two kinds of operation models [19]: 1) identification and 2) authentication. Shengrong Bu et al., [2011] 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). Based on a comparison of the matching score between the input sample and the enrolled template with a decision threshold, each biometric system outputs a binary decision: accept or reject. In most real-world implementations of biometric systems, biometric templates are stored in a location remote to the biometric sensors [7]. 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 frequencies of FA errors and of FR errors are 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 [19].

Authentication is a common prevention-based approach used in MANETs to reduce intrusions and also used to monitor computer networks and systems for violations of security and can be automatically performed by IDSs. Fundamentally, IDSs can be considered as network-based or host-based. Network-based IDSs are not suitable for MANETs since it needs to watch or gather data that run through the network hardware interface. Host-based IDSs, which rely on data generated by programs located on the host devices, are good candidates for MANETs [9]. Misuse detection and anomaly detection are two important aspects

in cluster based MANET to identifying intrusion because a malicious node can begin deny of service or interrupt the routing process by generating error. So the IDS is important in high security MANET to serve as a second wall of defence. The IDS constantly or periodically supervises the current subject activities, evaluates them with stored normal profiles and/or attack signatures, and begin appropriate responses.

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. The main drawback of misuse detection is that it cannot detect new forms of attacks. Anomaly detection is a behaviour-based method, which uses statistical analysis to find changes from baseline behaviour. This technology is weaker than misuse detection but has the benefit of catching the attacks without signature existence [11]. Multiple algorithms have been applied to model attack signatures or normal behaviour patterns of systems. Three common algorithms are specified in [8] such as 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 behaviour. DT, which is a useful machine learning technique, is used to organize the attack signatures into a tree structure. Most of the IDSs only use one of the preceding algorithms. IDSs can make two kinds of errors: false positive (FP) and false negative (FN). FNs result in security breaches since intrusions are not detected, and therefore, no alert is raised. The false negative rate (FNR) can be used to measure the secure characteristics of the IDSs since a low FNR implies a low possibility that intrusion occurs without detection [19] [22].

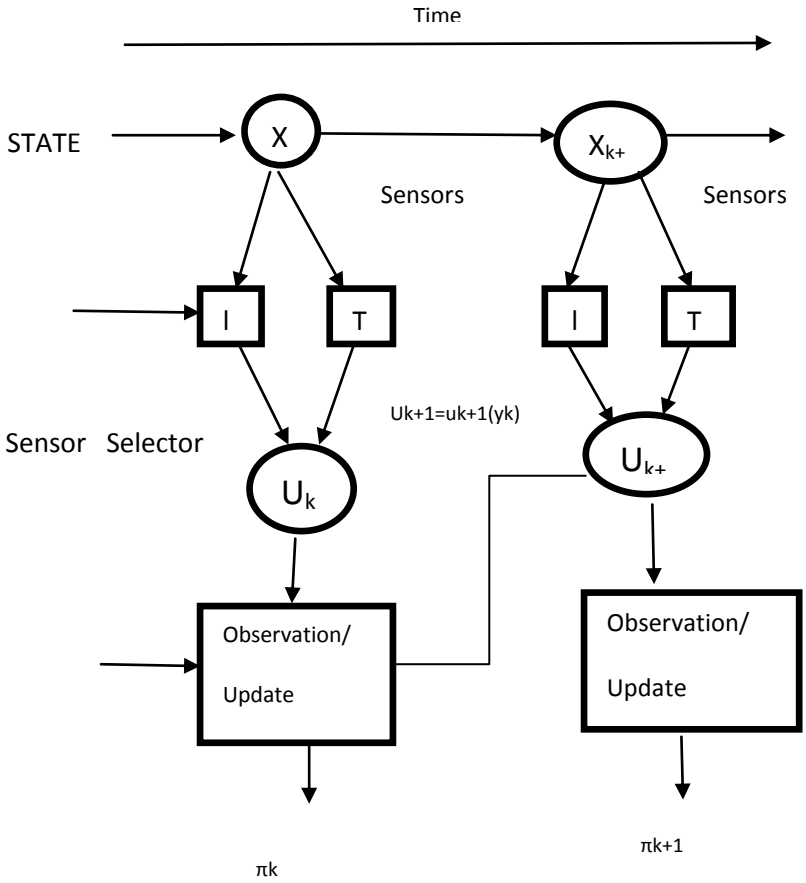

Fig. 1 Biosensor scheduling and information state update [11]

Multimodal Biometric System and Data Fusion: Multimodal Biometric is playing an important role in giving security between user-to-device authentications and it can be used in three operational modes such as serial, parallel and hierarchical. The output of one biometric attribute is used to narrow down the number of probable uniqueness before the next attribute is used in the serial multimodal system. In a parallel scheme of operation information from multiple behaviours are used at the same time to achieve gratitude. In the hierarchical multimodal, each and every classifier is combined in a treelike structure. IDS and response systems should work together to meet the needs of MANETs. Authentication is an essential type of responses initiated by IDS. Authentic users can continue to using the network resources only after the process of authentication and compromised users will be excluded [20]. Multimodal system gives the opportunity to gather all the needs of authentication and Dempster-Shafer theory is used for IDS and biometric sensors fusion in clustered MANETs. D. Ruta and B. Gabrys classified fusion methods as follows based

on the output information level of the base classifiers [9]: Type-I classifiers output single-class labels (SCLs). *Majority voting* and *behavior-knowledge space* are two methods for fusing SCL classifiers. Majority voting can operate under the assumption that most of the observing nodes are trustworthy. Type-II classifiers output class rankings. Two major fusion methods of type-II classifiers' outputs are based on either a class set reduction (CSR) or 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. Type-III classifiers produce so-called soft outputs, which are the real values in the range [0, 1]. Fusion methods for type-III classifiers try to reduce the uncertain level and maximize suitable measurements of evidence. Fusion methods include Bayesian fusion methods, fuzzy integrals, Dempster–Shafer combination, fuzzy templates, product of experts, and ANNs. The proposed system used the Dempster–Shafer theory for data fusion [19].

V. CONCLUSION

In the process of wireless network theory, the mobile ad hoc network security has revealed of wireless network. One of the important security aspects of MANET is authentication of ids and it has been devoted to develop algorithms that efficiently highlight the security of ad hoc network. Many cluster hierarchy algorithms have been proposed to solve the security issue. Only the authentic users can continue using the network resources after completion of an authentication process and compromised users will be excluded. Multimodal biometrics offers the possibility to meet all the requirements of authentication and Dempster-Shafer theory is used for IDS and biometric sensors fusion in clustered MANETs. Since there is more than one device used at each time slot and the WCA based cluster head selection algorithm used to select the high battery power CH in MANET.

REFERENCES

[1] Q. Xiao, "A Biometric Authentication Approach For High Security Adhoc Networks," In *Proc. IEEE Info. Assurance Workshop*, (West Point,NY), June 2004.

[2] J. Koreman, A. C. Morris, D. Wu, And S. A. Jassim, "Multi-Modal Biometrics Authentication On The Secure Phone Pda," In *Proc. Second Workshop On Multimodal User Authentication*, (Toulouse, France),May 2006.

[3] S. K. Das, A. Agah, And K. Basu, "Security In Wireless Mobile And Sensor Networks," *Wireless Communications Systems And Networks*, Pp. 531–557, 2004.

[4] J. Douceur, "The Sybil Attack," In *First International Workshop On Peer-To-Peer Systems (IPTPS'02)*, Cambridge, 2002, Pp. 251-260.

[5] Kuldeep Sharma, Neha Khandelwal, And Prabhakar.M, "An Overview Of Security Problems In MANET," In *Proceedings Of The International Conference On Network Protocols (ICNP)*, Kyoto, 2010.

[6] 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.

[7] A. Papanikolaou, C. Ilioudis, C. Georgiadis, And E. Pimenidis, "The Importance Of Biometric Sensor Continuous Secure Monitoring," In *Proc. 3rd Int. Conf. Digital Inf. Manage*, London, U.K., Nov-2008.

[8] C. Katar, "Combining Multiple Techniques For Intrusion Detection," *IJCSNS Int. J. Comput. Sci. Netw- Security*, Vol. 6, No. 2B, Pp. 208–218, Feb. 2006.

[9] D. Ruta and B. Gabrys, "An Overview Of Classifier Fusion Methods," *Comput. Inf. Syst.*, Vol. 7, Pp. 1–10, 2000.

[10] Ratish Agarwal And Mahesh Motwani., [2009], *"Survey Of Clustering Algorithms For MANET",* International Journal On Computer Science And Engineering Vol. 1(2), Pp. 98-104.

[11] Jie Liu, F. Richard Yu, Chung-Horng Lung And Helen Tang‡, "Optimal Biometric-Based Continuous Authentication In Mobile Ad Hoc Networks", Third IEEE International Conference On Wireless And Mobile Computing, Networking And Communications (Wimob 2007) 0-7695-2889-9/07,© 2007, IEEE.

[12] R.M.Chamundeeswari And Dr.P.Sumathi ," PERFORMANCE STUDY OF INTRUSION DETECTION TECHNIQUES IN MOBILE AD HOC NETWORKS", *International Journal Of Engineering And Techniques – Volume 1 Issue 2, Mar – Apr 2015.*

[13] Azin Moradmand Badie, Dale Lindskog And Ron Ruhl, "Responding To Intrusions In Mobile Ad Hoc Networks", World Congress On Internet Security (Worldcis-2013), 978-1-908320-22/3©2013 IEEE.

[14] Ramalingam. M., Thiagarasu.V., [2014], *"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,Vol.3,No.10,Pp.392-400.

[15] Bo YANG, Ryo YAMAMOTO And Yoshiaki TANAKA," 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, Issue 3, May 2013,Isbn:978-89-968650-3-2,Copyright: Giri (Global IT Research Institute).

[16] Rajakumar.P, Prasanna Venkatesan T And Pitchaikkannu.A," Security Attacks And Detection Schemes In Manet", Dept. Of Information Technology ,Anna University, RC,Coimbatore – 641047.

[17] Ajay Jangra And Shivi Goel," Biometric Based Security Solutions For MANET: A Review", *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.

[18] Mohammed M. Alani," MANET Security: A Survey", 2014 IEEE International Conference On Control System, Computing And Engineering, 28 - 30 November 2014, Penang, Malaysia, 978-1-4799-5686-9/14, ©2014 IEEE.

[19] Shengrong Bu And F. Richard Yu, "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, 0018-9545, © 2011 IEEE, MARCH 2011.

[20] 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", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 2, 1536-1276/09$25.00 _C 2009 IEEE, FEBRUARY 2009.

[21] Pushpita Chatterjee," TRUST BASED CLUSTERING AND SECURE ROUTING SCHEME FOR MOBILE AD HOC NETWORKS", International Journal Of Computer Networks & Communications (IJCNC), Vol.1, No.2, July 2009.

[22] 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", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 2, 1536-1276/09, 2009 IEEE.

[23] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks," in *Proceedings of the 42nd annual Southeast regional conference (ACMSE'04)*, Huntsville, 2004, pp. 96-97.