© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

# Stretch and Shrink Method for Security in MANET Using Biometric and Intrusion Detection System

**Dr. P. Prabhusundhar*, Dr. B. Srinivasan, Dr. M. Ramalingam**
Assistant Professor, Computer Science Gobi Arts & Science College (Autonomous) Gobichettipalayam, Tamilnadu, India

## ABSTRACT

Mobile ad hoc is an infrastructure less dynamic network used in many applications; it has been target of various attacks and it makes security problems. The MANET is a collection of autonomous wireless nodes, in which each node changes its geographical position frequently and acts as a router to forward packets. 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 scheme, Dempster-Shafer theory is used for data fusion because more than one device needs to be chosen and their observation can be fused to increase observation accuracy. The topology stability and network scalability are playing a significant role in mobile ad hoc to determining the network performance. Hence an attempt has been made to analyze the factors such as nearest neighbor and association rule mining in the ad hoc network's bench mark algorithms such as LCA2, load balance, adaptive multi-hop algorithm and Basagni's DCA and DMAC to form a clustered mobile ad hoc network.

**Keywords:** MANET, WCA, rule mining, stretch and shrink, 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. MANET is unlike fixed hardwired networks with physical defense 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 node must be prepared to encounter with an adversary directly or indirectly. 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 have identified by their physiological characteristics.

**Table 1**. Active And Passive Attacks

| | |
|---|---|
| **Active Attacks** | Spoofing |
| | Fabrication |
| | Wormhole Attack |
| | Modification |
| | Denial of Service |
| | Denial of Service |
| | Black holes and Gray holes |
| | Sybil Attack |
| **Passive Attacks** | Eavesdropping |
| | Monitoring |
| | Traffic Analysis |

Malicious activities by misbehavior node can be efficiently identified by intrusion detection systems (IDSs). IDSs can be classified in to three types: (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 neighbor. 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. 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. 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). 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.

## II. UNIMODAL BIOMETRIC SYSTEM

Unimodal Biometric system depends on single biometric trait. Single biometric trait is used for person's identification or verification. This system is used for various applications. It is also used for the security purpose. Though the system has a wide range of application it can be affected by following drawbacks. Noisy Data: Due to noisy data the matching is inaccurate that leads to false rejection. Intra class variation: Intra class variation increases the false rejection rate. It is occurred due to the biometric data acquired is not same as the data used to create the template. Inter class similarities: Inter class similarities are due to the overlapping of feature space due to multiple individuals. It leads to increase the FAR (False Acceptance Rate). Non-universalities: Due to illness or disability some persons cannot provide required biometric.

Distinctiveness: Inter-user similarity refers to the overlap of the biometric samples from two different individuals in the feature space. Biometric trait is expected to vary significantly among individuals; there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discrimination power provided by the biometric trait. Spoofing: An individual may use fake the biometric trait. It is easy for behavioral characteristics, such as when signature and voice are used as an identifier. To overcome these drawbacks Multimodal Biometric system is used [Rupali L, Telgad et al., 2014].

A unimodal fingerprint verification and classification system is presented by [Prabhakar, et al., 1998]. The system is based on a feedback path for the feature-extraction stage, followed by a feature-refinement stage to improve the matching performance. This improvement is illustrated in the contest of a minutiae-based fingerprint verification system. The Gabor filter is applied to the input image to improve its quality. Ratha et al., [2000] proposed a unimodal distortion-tolerant fingerprint authentication technique based on graph representation. Using the fingerprint minutiae features, a weighted graph of minutiae is constructed for both the query fingerprint and the reference fingerprint.

Concerning iris recognition systems in feature [Vincenzo Conti et al., 2010], the Gabor filter and 2-D wavelet filter are used for feature extraction. This method is invariant to translation and rotation and is tolerant to illumination. The classification rate on using the Gabor is 98.3% and the accuracy with wavelet is 82.51% on the Institute of Automation of the Chinese Academy of Sciences (CASIA) database. In the approach proposed by [L. Ma,Y.Wang and D. Zhang, 2004], multichannel and Gabor filters have been used to capture local texture information of the iris, which are used to construct a fixed-length feature vector. The results are FAR = 0.01% and FRR = 2.17% in CASIA database. Generally, unimodal biometric recognition systems present different drawbacks due its dependency on the unique biometric feature [Vincenzo Conti et al., 2010].

## III. LIMITATIONS OF UNIMODAL BIOMETRIC SYSTEMS

Most biometric systems deployed in real-world applications are unimodal, so they rely on the evidence of a single source of information for authentication. These systems have to contend with a variety of problems such as noise in sensed data, intra-class variations, inter-class similarities and spoof attacks [Salah M. Rahal et al., 2006].

**Biometrics vs Passwords:** First, the security of a password-based authentication tool such as ones in UNIX or Windows systems are based on the local storage of only cryptographic hashes of passwords, no passwords themselves. This is possible because of the deterministic nature of password authentication: if the entered candidate password is the correct then its hash value equals the stored hash value and the

authentication succeeds; if the entered candidate password is a wrong then its hash value differs and the authentication fails. Such an approach of security is impossible with biometric data.

Any new capture of a biometric candidate results in slightly different data, which leads to the statistical nature of Biometrics based authentication (distance evaluation between two samples). The hash value of a reference biometric template will be totally different from the hash value of any matching candidate. This means that biometric references have to be stored in clear text.

A deep characteristics analysis of both passwords and biometrics shows a clear apposition:

- Secrecy: A password/PIN code is a secret, whereas biometric data is public. However, have to make here a distinction between biometrics leaving traces (e.g. fingerprints) and others (e.g. hand geometry).
- Delegation: Depending on the application, the delegation ability is mandatory (banking, mobile communications) or must be impossible (civilian identification documents).
- Changeability: In case of compromise, a password is denied and another one is issued. It is not that easy with biometrics.
- Personalization: A PIN code is mailed (e.g. banking), whereas biometrics request user's Enrollment (i.e. the user has to go in a security area of the registration authority).
- Comparison process: The comparison between two PIN codes is a very simple task for a smart card, whereas comparing fingerprints needs far more computation resources.
- User convenience: A PIN code must be memorized and often manage several PIN codes, whereas biometrics need no effort.
- Vulnerability to eavesdropping: A discrete monitoring the actions could reveal the password, whereas biometric data cannot be copied.
- Vulnerability to brute force attack: Passwords are few characters long, whereas a biometric template is few hundreds of bytes.
- Countermeasures: Attacks against PIN code and passwords are experienced for many years and countermeasures are mature. Attacks against biometric systems are a novel area with no mature countermeasures for the time being.
- "Real" user authentication: User authentication with PIN code is only a legal trick: the law says "this PIN code is personal, do not share it". Biometrics is a stronger link with the user himself
- Capture: Entering a PIN code is simple (small keyboard), whereas capturing a biometric trait is an expensive task (cost and maintenance of a reader)

This opposition confirms the good complementarity of passwords and biometrics. The replacement of one with the other should be carefully studied depending on the targeted application. Despite the aforementioned vulnerabilities of biometrics, it should be counterbalanced with situations where biometrics is more secure than passwords: weak passwords, bad managed passwords, password-based authentication deactivated by the user.

Many information system administrators complain about users writing their password on a Post-It R note stuck under their keyboard or even on their computer's screen. Many mobile phone users leave the default PIN code (e.g. 0000, 1234) to unlock the phone or even deactivate this security feature considered as counter user convenient. Too many passwords, to be memorized, are short and explicit hence it could be easily guessed with simple dictionary attack or more sophisticated attacks. [Claude BARRAL 2010]. The various characteristics of biometric and password are listed in Table 2.

**Table 2.** Biometrics Vs Passwords [Claude Barral 2010]

| Characteristics | PIN code | Biometrics |
|---|---|---|
| Secrecy | Secret | Public |
| Delegation ability | Yes | No |
| Changeability | Yes | No |
| Personalization | Easy | Difficult |
| Comparison process | Simple | Not so trivial |
| User convenience | No | Yes |
| Vulnerability to Eavesdropping | Yes | No |
| Vulnerability to Brute Force attack | Yes | Not so trivial |
| Attacks countermeasures | Mature | Immature |
| "Real" user authentication | No | Yes |
| Capture | Easy | Expensive |

## IV. IDS SYSTEM

Intrusion detection system (IDS) 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. 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 behavior-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 of 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, checkup 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 behavior and then defining at all other behavior 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 system can only observe 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.

**Bayes-Adaptive POMDP:** St´ephane Ross introduced the Bayes-Adaptive POMDP (BAPOMDP) model, an optimal decision theoretic algorithm for learning and planning in POMDPs under parameter uncertainty. Throughout assume that the state, action and observation spaces are finite and known, but that the transition and observation probabilities are unknown or partially known. Also assume that the reward function is known as it is generally specified by the user for the specific task he wants to accomplish, but the model can easily be generalized to learn the reward function as well [St´ephane Ross et al.,].

## V. THE STRETCH AND SHRINK METHOD

The nearest neighbor method is used in the ad hoc network to divide the nodes in to number of groups or clusters.

The clustered network can be shrinking (split) or stretch (merge) based on the threshold value and association rule mining. If the current cluster's node density is greater than the threshold value, the cluster can be shrinking as well as the cluster can be stretch when the cluster node density is smaller than the threshold (pre-defined) value. The above two process of stretch and shrink can be done by using the nearest neighbor method.

Threshold is a predefined value that a cluster can cover. The threshold value decides whether to add a new node to the existing cluster or not.

The load balancing cluster concept in ad hoc network is accomplished by determining a predefined threshold on the number of nodes that a cluster head can cover ideally.

So the threshold helps to balance the nodes in the network and none of the cluster heads are overloaded. Abdel Rahman H et al., 2009, uses the pre-defined threshold value as 5 nodes in each cluster.

The load balancing method plays an essential role in ad hoc network to minimize the cluster head overhead and make topology stability and the bench mark algorithms (DCA, DMAC, DLBC, ACM) has been used in this method by setting the upper threshold limit and lower threshold limit in each cluster to maintain the balanced nodes in ad hoc network.

So the cluster head overload is minimized as well as the topology change [Ramalingam M. et al.,].

## VI. CONCLUSION AND FUTURE RESEARCH

In this paper, three data mining techniques and ad hoc load balanced benchmark algorithms have been analyzed which uses the load balance method, cluster, nearest neighbor, rule mining and threshold value to form a balanced clustered ad hoc network. By using the nearest neighbor to form an effective cluster in ad hoc and the rule mining, threshold predefined value techniques have to maintain the balanced nodes in organization of a mobile radio network. The biometric security system discussed the general architecture of a biometric system and various mobile ad hoc network attacks. The three primary

components of security such as authentication, authorization and accountability are used in the biometric security. The attacks can be classified into the five categories such as black hole, byzantine, wormhole, spoofing attack and sybil attack. Cluster based intrusion detection and prevention technique, fingerprint and iris recognition are also discussed in biometric technology. The system also reviewed multimodal biometric schemes and four slap fingerprint scanner to simultaneously collect fingerprints of multiple fingers on a hand in one image.

## VII. REFERENCES


[1]. Chengyu liu, lina zhao," A new algorithm of nodes partition using for ad hoc network model", proceedings of ieee ic-bnmt2011, 978-1-61284-159- 5, 2011-ieee

[2]. Jahangir khan, Dr.syed Irfan Hyder, Dr.Syed Malek Fakar Duani syed Mustafa , International Journal of Grid and Distributed Computing, "Modeling and Simulation Of Dynamic Intermediate Nodes And Performance Analysis in MANETS Reactive Routing protocols" Vol. 4, No. 1, March 2011

[3]. Ramalingam. M, Dr.Thiagarasu.V , Narendran.P, "Periodical and On-Demand Topology Dissemination in routing protocols: A comprehensive Analysis based on Delay, Delivery Ratio and Throughput", International Journal of Advanced and Innovative Research (2278-7844) / # 123 / Volume 2 Issue 9, 2013

[4]. C. E. Perkins, E. M. Royer, S. R. Das, M. K. Marina. "Performance comparison of two on-demand routing protocols for ad hoc networks", IEEE Personal Communications, 2001, 2: 16-28

[5]. Ratish Agarwal, Roopam Gupta, and Mahesh Motwani," Energy Aware Load Balancing Clustering in Mobile Ad Hoc Networks", International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 2, Issue 1 (2014) ISSN 2320-401X; EISSN 2320-4028

[6]. Yi Xu and Wenye Wang, "Topology Stability Analysis and Its Application in Hierarchical Mobile Ad Hoc Networks", IEEE transactions on vehicular technology, vol. 58, no: 3, march 2009

[7]. Prerna Malhotra, Ajay Dureja, "A Survey of Weight-Based Clustering Algorithms in MANET", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 34-40 8D.J.Baker and A. Ephremides, "The architectural

[8]. A. D. Amis and R. Prakash, "Load-Balancing Clusters in Wireless Ad Hoc Networks", in Proc. 3rd IEEE ASSET'00, Mar. 2000, pp. 25–32

[9]. ChetnaKaushal, Naveen Bilandi, "A Review: Clumping in Mobile Ad hoc Networks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2014, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798

[10]. Abdel Rahman H. Hussein, Sufian Yousef, and Omar Arabiyat," A Load-Balancing and Weighted Clustering Algorithm in Mobile Ad-Hoc Network", IT Security conference for the Next Generation, University of East London, London, UK, Vovember21-22-2009

[11]. A. Ephremides, J. E. Wieselthier, and D. J. Baker," A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling", Proceedings of IEEE, 75(1):56–73, 1987

[12]. D.J. Baker and A. Ephremides, "A distributed algorithm for organizing mobile Radio telecommunication networks", in: Proceedings of the 2nd International Conference on Distributed Computer Systems, April 1981, pp. 476–483

[13]. Ratish Agarwal, Dr. Mahesh Motwani, "Survey of clustering algorithms for MANET", Ratish Agarwal.et al, International Journal on Computer Science and Engineering Vol.1(2), 2009, 98-104

[14]. M. Gerla and J. T. Tsai, "Multiuser, Mobile, Multimedia Radio Network," Wireless Networks, vol.1, Oct. 1995, pp. 255–265.

[15]. A.K. Parekh, "Selecting routers in ad-hoc wireless networks", in: Proceedings of the SBT/IEEE International Telecommunications Symposium, August 1994.

[16]. Ramalingam M and Dr. 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.

[17]. Prabhusundhar P and Dr. Srinivasan B., 2016], "Multimodal Biometric and Weighted Clustering Algorithm for Authentication Based Intrusion Detection System for Clustered MANET Using POMDP", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), ISSN (Online): 2277 128X, ISSN (Print): 2277 6451, Vol. 6, No. 3, March-2016.

[18]. Prabhusundhar P and Dr. Srinivasan B., 2016], "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.

[19]. Aarti and Tyagi S.S., 2013], "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3(5), pp. 252-257.

[20]. Adnan Nadeem, Michael and Howarth., "An Intrusion Detection & Adaptive Response Mechanism for MANETs", Journal of Elsevier.

[21]. Aguilar G, Sanchez G, Toscano K, Nakano M and Perez H., 2007], "Multimodal Biometric System using Fingerprint", in the proceedings of Int. Conf. Intell. Adv. Syst. 2007, DOI: 10.1109/ICIAS.2007.4658364, pp. 145-150.

[22]. 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..