Intrusion Detection and Continuous Authentication using Multimodal Biometrics in MANETS – A Survey

M.Ambika
PG Scholar
Dept of IT
Bannari Amman Institute of Technology,
Sathyamangalam

R.V.Nataraj
Professor
Dept of IT
Bannari Amman Institute of Technology,
Sathyamangalam

ABSTRACT

Mobile ad hoc networks (MANET) have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. The mobile nodes are exposed to various kinds of attacks and most of the times the intruders get into network, in order to hold illegal authority over the nodes. Multimodal biometric technology provides potential solutions for continuous user-to-device authentication in high security mobile ad hoc networks. Intrusion detection is considered as the prevention based approach for securing the MANETs. This paper aims to classify various intrusion detection techniques used in MANETs. Also this paper showcases process of continuous authentication through multimodal biometric technique.

Keywords

Mobile Ad hoc Networks, Intrusion detection, Multimodal Biometrics, Intruders

1. INTRODUCTION

A Mobile Adhoc Network (MANET) is a collection of mobile hosts that can communicate with each other without any pre-established infrastructure. Each node in the MANET can act as router as well as host. For maintaining the connectivity among the nodes in the entire mobile ad hoc network routing of network traffic is necessary. Co-operation from the nodes are very important from all the nodes in the network. Therefore, MANET has the property of rapid infrastructure-less deployment and no centralized controller which makes it convenient to many environments, such as battlefield, emergency disaster relief and business meeting. Due to inherent characteristics of MANETs, it is subject to different vulnerabilities. The main disadvantage in MANET protocol is that the nodes are assumed to work in a co-operative network which is not possible always. Fig. 1 shows a simple Mobile Ad hoc Network structure:

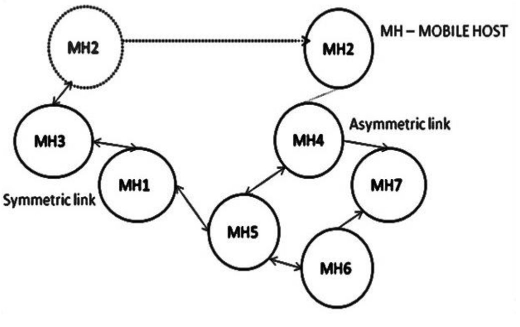

Fig 1: A mobile ad hoc network (MANET)

The mobile ad hoc network have many salient characteristics such as dynamic topology, bandwidth constrained, variable link capacity, limited energy, limited physical security [1]. Due to these characteristics the MANETs are vulnerable to various malicious attacks.

User authentication is very important for authenticating the legitimate users, and preventing the adversaries from entering into the network. Multimodal biometrics technology can be employed in each mobile node for continuous authentication.

Intrusion detection (ID) is another security mechanism which is used to identify those who are trying to break and misuse the system without authorization and those who have legitimate access to the system but misusing the privileges.

The organization of this paper is as follows. In section 2 presents the recent scenario of intrusion Detection System. In section 3 various intrusion detection techniques are discussed and finally. Section 4 concludes the survey article and finally the references are included in section 5.

2. BIOMETRIC-BASED USER AUTHENTICATION

Biometrics is an automatic identification or verification of an individual by his or her physiological or behavioral characteristics. Biometrics provides a possible solution to authentication in MANETs, because it has a direct connection with the user identity, can be continuously monitored, and needs little user interruption [2].

Each biometric technology has its own strengths and weaknesses. Unimodal biometrics has to face several challenges such as noise in sensed data, intra-class variations, inter-class similarities, etc. [3]. Multimodal biometric systems present more reliable authentication methods due to the combination of statistically independent biometric traits [4]. These systems can exploit the benefits of one biometric and mitigate the shortcomings of another biometric.

There are three different modes of system operation in multimodal biometrics system: serial mode, parallel mode, and hierarchical mode [3]. In serial mode of operation, one output of a biosensor will be used at one time. Therefore, multimodal biometric traits do not need to be acquired simultaneously, and the decision could be made before all biometric traits are received. The overall recognition time can be reduced, which is important for MANETs. In the parallel mode of operation, multimodal biometric traits have to be used simultaneously. The hierarchical mode of operation is suitable for the system using a large number of biometric traits. This paper will consider the serial mode of operation since it is suitable for continuous authentication in MANETs.

2.1 Normal or Body Text Continuous Verification Using Multimodal Biometrics

The goal is to have T. Sim et. al. [5] proposed a continuous biometric authentication. The system was a multimodal biometric verification system which continuously verifies the presence of a logged-in user. This system adds an extra overhead on the requirements of multimodal fusion when compared to the conventional verification systems. The integration scheme used in this system is shown in Fig.2:

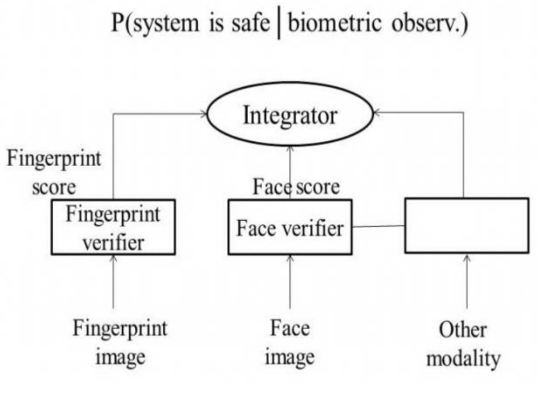

Fig 2: Integration scheme

The system was also sufficient for high-security environments in which the protected resources needs to be continuously monitored for use [6]. This method is addressed for the biometric-based continuous authentication based Secure Phone mobile communication system. This system gave access to e-signing, m-contracts in a secured authenticated approach. Based on several test using fusion techniques for biometric evidence combination, an efficient multi-modal biometric authentication was achieved on the Secure Phone PDA. The weighted error rate for the fusion technique is given by:

$$p(s|C)=\sum_{i=1}^{N}\alpha_i N(s,\mu_i,\sum i)$$

2.2 Temporal Integration for Continuous Multimodal Biometrics

Altinok et. al. [7] proposed a multimodal system that performs authentication continuously by integrating the information temporally as well as across modalities. The proposed modal [7] also has another advantage of providing ongoing verification and can easily be coupled with another system for dynamically adjusting the access to privileges accordingly. The system operates continuously by computing expected values as a function of time differences.

The temporal integration method that depends on the availability of past observations [8] addressed the issue of post-login user verification using multimodal approach of dynamic Bayesian networks. The proposed framework [8] provides continuous verification of user identity by monitoring the user characteristics throughout the session. Another main advantage of the system is the system can also be extended to include important contextual information. Tests were performed using face recognition and keystroke dynamic and results show a promise and warrant future work to develop more controlled experiments for use of additional modalities to improve the robustness of the system.

3. INTRUSION DETECTION TECHNIQUES IN MANET

Most of the traditional methods like encryption and authentication involved in the process of intrusion prevention are not sufficient for the first line of defense. Once the system becomes more complicated, there are also more weaknesses that lead to numerous security problems. Intrusion detection can be used as a second layer of defense against the attacks rising in the network. If the intrusion is detected, a warning can be initiated to prevent or minimize the damages to the system.

Intrusion detection may be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified as anomaly detection systems, Misuse detection systems; Specification based design [9].

3.1 Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks

Nakayama et al. [10] have proposed a new anomaly detection model for MANET. This, model aims at detecting the malicious behaviors of Ad-hoc On-demand Distance Vector (AODV) [11] routing protocol. This model uses the machine learning technique in order to generate and maintain a normal profile and relies on principal component analysis (PCA) for resolving malicious behaviors. During the learning phase this system collects the packets from network traffic and maintains the normal profile. During the monitoring phase the features are collected within the fixed time interval of five seconds. The recorded features are expressed by p dimension vector. Using PCA on the normal profile, the first principal component is calculated, which reflects an approximate distribution of the normal profile. The first principal component is the linear combination of the original variables with the largest variance.

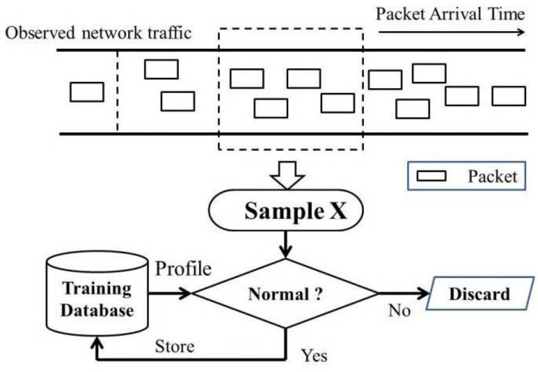

Fig 3: Flowchart of the proposed method for learning and evaluation

On the other hand, by applying PCA on the collected data of the first monitored time slot, the deviation from the first principal component can be estimated. If this deviation exceeds aM, the engine assumes that an attack takes place. Otherwise, the recorded data from the monitored time becomes the new normal profile. The low rate of false positive alarms caused by dynamic network changes is a great advantage of this method. This is achieved by dynamically updating the normal profile at runtime. But this method cannot be used to detect all type of attacks because it monitors features only at the network layer.

3.2 Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks

Shengrong Bu et al. [12] proposed a fully distributed scheme of combining intrusion detection and continuous authentication in MANETs. Distinct features of the proposed scheme are:

1) In the proposed scheme, multimodal biometrics is deployed to alleviate the shortcomings of unimodal biometric systems.

2) Since each device in the network has measurement and estimation limitations, more than one device can be chosen, and their observations can be fused to increase observation accuracy. Dempster–Shafer theory is used for data fusion.

3) The system decides whether a user authentication (or IDS) is required and which biosensors (or IDS) should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IDS. Since there is no need for centralized controller, the proposed scheme is more generic and flexible than a centralized scheme in MANETs. Nodes can freely join and leave from the network.

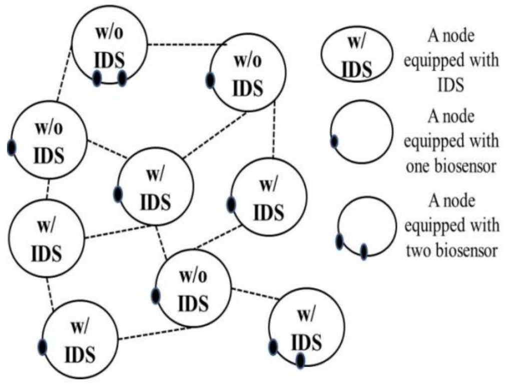

Fig 4: Example framework for a MANET with biosensors and IDs

4) Since a biometric authentication process requires a large amount of computation, the energy consumption is significant. Moreover, due to the dynamic wireless channels in MANETs, the energy consumption for data transmissions is dynamically changing (e.g., because of power control). Therefore, in the proposed scheme, energy consumption is also considered to improve the network lifetime. The problem has been formulated as a POMDP multiarmed bandit problem. The communication overhead of the proposed algorithm is O (LN).The main strength of the above system is the combination of authentication and intrusion detection. Computational complexity is considered to be the major drawback of this technique.

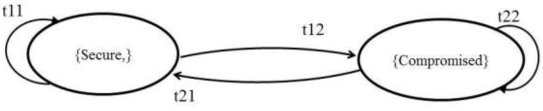

Fig 5: Example of Markov chain for a single node’s state transition

3.3 Design-Based Secure Leader Election Model for Intrusion Detection in MANET

Noman Mohammed et al. [13] proposed a mechanism design based model for secure leader election in the presence of selfish nodes. The most remaining resources is elected as the leaders for balancing the resource consumption of the nodes in the network nodes.

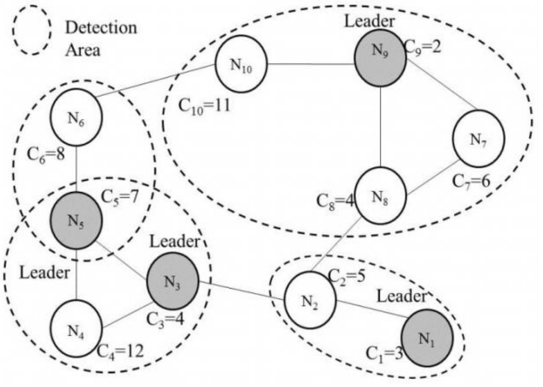

Fig 6: Reputation System Model

In order to elect the leader, the nodes which are honestly participating in the election process are provided with incentives. The amount of incentives is based on theickrey, Clarke, and Groves (VCG) model. This model proposed a two leader election algorithms namely Cluster dependent Leader Election (CDLE) and Cluster Independent Leader Election (CILE). The former does not require any preclustering whereas CDLE requires nodes to be clustered before running the election mechanism.

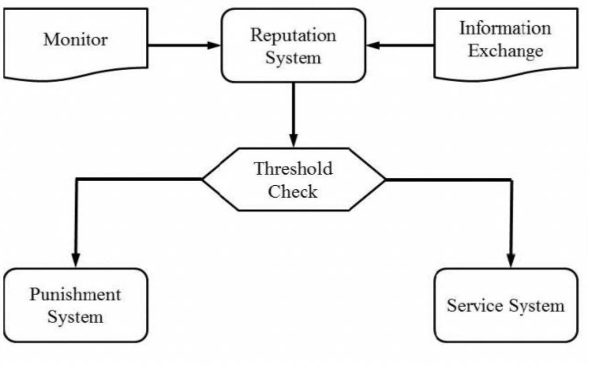

Fig 7: Example of Leader Election

Simulation results showed that their model is able to prolong the lifetime and balance the overall resource consumptions among all the nodes in the network. To elect the leaders number of tables need to be maintained and also different messages need to be transferred between nodes of the network. The main drawback of this model is the creation of performance overhead and storage overhead in clustering.

3.4 Evolutionary Computation Techniques for Intrusion Detection in MANETs

Sevil Sen and John A.Clark [14] used an evolutionary computation (EC) techniques particularly genetic programming (GP) and grammatical evolution (GE) to evolve intrusion detection programs. Also they analyzed the power consumption of evolved programs. They formed a multi objective evolutionary algorithm to discover optimal tradeoffs between intrusion detection ability and power consumption.EC techniques are proposed to discover the complex properties of MANETs.

The mobility and packet related features are used as an input to the detection algorithm. In GP a problem is defined with functions and terminals which are parts of a GP tree and the fitness function. Fitness function is used a metrics to evaluate an IDS. In GE, a problem is defined with a grammar and a fitness function. They used ECJ18 toolkit and libge library for implementing GP and GE. They monitored the performance measures such as detection rate and false positive rate by varying mobility and traffic load. The main strength of this approach is it uses the evolutionary computing which is light weight compared to other machine learning technique. This model uses only the network layer features so it is not possible to detect the attacks present in the remaining layers.

4. CONCLUSION

Intrusion detection system for mobile ad hoc networks has attracted much attention recently due to increased usage of mobile ad hoc networks. There are many IDS solutions are proposed or improvements made in the existing one. This paper has evaluated and compared the latest and most prominent IDS architectures for MANETs. Based on the carried analysis, it can be deduced that the existing IDS architectures for MANETs present significant limitations and weaknesses. Most of the detection engines work on a limited set of features in order to make their deployment computationally feasible on MANETs. Therefore, detecting all these types of attacks is not possible. Some of the techniques use multiple layer features but the large set of features increase the overhead. The performance metrics of several proposed engines is negatively affected with respect to nodes' mobility and traffic load of a MANET. Reducing the computational complexity is a challenging issue of all the detection methods. There is a need of better tradeoff between performance and overhead of the detection system.

5. REFERENCES

[1] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology Vol. 11 No. 2.

[2] Q. Xiao, "A biometric authentication approach for high security ad-hocnetworks," in Proc. IEEE Info. Assurance Workshop, West Point, NY,June 2004.

[3] A. Ross and A. K. Jain, "Multimodal biometrics: an overview," in Proc.12th European Signal Proc. Conf., Vienna, Austria, 2004.

[4] A. Ross and A. K. Jain, "Information fusion in biometrics," PatternRecognition Lett., vol. 24, pp. 2115-2225, Sept. 2003.

[5] Sim T, Zhang S, R.Janakiraman and S.Kumar, "Continuous verification using multimodal biometrics," IEEE Trans. Pattern Anal. Mach. Intell.2007; vol. 29, pp. 687-700.

[6] Korman J, A C Morris, D Wu and S.A.Jassim, "Multi-modal biometrics authentication on the secure phone PDA," in Proc. 2nd Workshop Multimodal User Authentication, Toulouse, France, May 2006.

[7] Altinok A, M Turk, "Temporal integration for continuous multimodal biometrics," in Proc. Workshop Multimodal User Authentication, Santa Barbara, CA, Dec. 2003.

[8] Muncaster J, Turk M, "Continuous multimodal authentication using dynamic Bayesian networks," in Proc. 2nd Workshop Multimodal User Authentication, Toulouse, France, May 2006.

[9] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wire-less Ad Hoc Networks," *IEEE Wireless Communications*, Vol. 11, Issue 1, pp. 48-60, February 2004.

[10] H.Nakayama, S.Kurosawa, A.Jamalipour, Y. Nemoto, N.Kato, "A Dynamic Anomaly Detection Scheme for AODVBasedMobile Ad Hoc Networks," IEEE Transactions onVehicular Technology, vol.58, no.5, pp.2471-2481, Jun 2009.

[11] C.E. Perkins, E. M. Belding-Royer, and S. R.Das, "AdHoc On-Demand Distance Vector Routing", IETF RFC 3561,July 2003.

[12] S. Bu, F. Yu, X. Liu, P. Mason and H. Tang, "Distributedcombined authentication and intrusion detection with data fusionin high-security mobile ad hoc networks," IEEE Transactions onVehicular Technology, vol 60 no.3 pp. 1025–1036, March 2011.

[13] Noman Mohammed Hadi Otrok, Lingyu Wang, MouradDebbabi and Prabir Bhattacharya, "Mechanism Design-BasedSecure Leader Election Model for Intrusion Detection inMANET**"** IEEE Transactions on dependable and SecureComputing, vol 8, no 1, Jan-Feb 2011.

[14] Sevil Sen, John A. Clark "Evolutionary computationtechniques for intrusion detection in mobile ad hoc networks".Computer Networks Vol 55, Issue 15, pp. 3441-3457,211.