ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Authentication and Intrusion Detection System for Mobile Ad-Hoc Networks

R.Divya[1], N.Saravanan[2]

M.Tech, Department of IT, KSR College of Engineering, Thiruchengode, Tamilnadu, India[1]

Associate Professor, Department of IT, KSR College of Engineering, Thiruchengode, Tamilnadu, India[2]

ABSTRACT: Mobile ad-hoc network is an infrastructure less network. Continuous user authentication is an important prevention-based approach to protect the high security mobile ad-hoc networks (MANETs). Also intrusion detection systems (IDS) are also important in MANET to effectively identify malicious activities. Most previous work studies these two classes of issues separately. In this paper, we propose a framework of combining intrusion detection and continuous authentication in MANETs. In this framework, multimodal biometrics is used for continuous authentication and intrusion detection is modeled as sensors to detect system security state. To obtain the optimal scheme of combining continuous user authentication and IDSs in a distributed manner, we formulate the problem as a partially observable Markov decision process (POMDP) multi-armed bandit problem. We present a structural result method to solve the problem for large networks with number of nodes are used.

KEYWORDS- Security, Authentication, mobile ad-hoc network, IDS.

I. INTRODUCTION

With recent advances in mobile computing and wireless communications, mobile ad-hoc networks (MANETs) are becoming more attractive for use in various applications [1]. Mobile ad hoc network (MANETs) becomes a popular research subject due to their self-configuration and self-maintenance capabilities. Wireless nodes can establish a dynamic network without the need of a fixed infrastructure. This type of network is very useful in tactical operations where there is no communication infrastructure. However, security is a major concern for providing trusted communications in a potentially hostile environment. Two classes of approaches, prevention based such as user authentication and detection-based such as intrusion detection can be used to protect high security MANETs. User authentication is critical in preventing non authorized users from accessing or modifying network resources in high security MANETs. User authentication needs to be performed continuously and frequently, since the chance of a device in a hostile environment being captured is extremely high [2]. User authentication is critical for integrity, confidentiality and non-repudiation [3], [4]. Authentication can be performed by using one or more of the following validation factors something a user knows, such as a password; something a user has, such as a token or a smart card and something a user is, such as a fingerprint or iris pattern [5].

Biometrics technology, such as the recognition of fingerprints, irises, retinas, etc., provides some possible solutions to the continuous user authentication problem in MANETs [6], since it has direct connection with user identity. Intrusion detection systems (IDSs) are also important in high security MANETs to effectively identify malicious activities. In the MANETs, Host-based IDSs are suitable since no centralized gateway or router exists in the networks [7].

Multimodal biometrics can be used to alleviate some drawbacks of one mode of biometrics by providing multiple verifications of the same identity [8]. Many efforts have been made to research on either continuous user authentications or host-based intrusion detection systems. Continuous authentication and intrusion detection can be considered jointly to further improve the performance of high security MANETs. The authors in [9] proposed a useful framework to combine the user authentication and intrusion detection. The proposed scheme in [9] is a centralized scheme, in which the whole network is formulated as a single partially observable Markov decision process (POMDP). Solving the POMDP can be computationally intractable since the state space of the POMDP grows exponentially with the number of biometric sensors and IDSs [10].

Both continuous authentication and intrusion detection may consume extensive system resources. System resource constraints are important issues in MANETs. Some examples of the constraints include limited battery power, low-power microprocessor and small memory. Considering these two processes jointly will be helpful to optimally allocate resources in MANETs. A common framework to enable continuous authentication and intrusion detection jointly may result in a more complex system than designing them separately. The system should be carefully designed taking into account of system security requirements and resource constraints.

II. RELATED WORKS

Continuous user authentication and intrusion detection in MANETs, these two important areas have traditionally been addressed separately in the literature. In this paper, we propose to use a common framework to enable continuous authentication and intrusion detection jointly and make them share information with each other so as to obtain more efficient and cost effective mechanisms for these two processes. It is generally assumed that authentication decisions should be based only on the outcome from the authentication systems (e.g., fingerprint), and intrusion detection. However, the purpose of continuous authentication is to check the system security state (safe or compromised) which is also the main purpose of intrusion detection. Therefore, the information to solve one problem may be useful to solve another one. If a sensor is chosen, its information state at that time can be updated using the hidden Markov model state filter with the new observation. Otherwise, their information states remain unchanged at that time slot. Therefore, the above POMDP multi-armed bandit problem can be re-expressed as a fully observable multi-armed bandit problem in terms of the information state which means the optimal sensor can be chosen based on the information state.

Each biometric technology has its own strengths and weaknesses. For example, iris pattern is more accurate than voice identification, but getting a good image of the iris is difficult. Signature is a widely accepted authentication method, but it still remains a question if it could acquire the same level accuracy as the other biometric technologies. Currently, there is no best biometric modality since it depends on the environment applied. Unimodal biometrics has to face several challenges such as noise in sensed data, intra-class variations, inter-class similarities, etc [11]. Some of these problems could be resolved by adopting multimodal biometric systems. Multimodal biometric systems present more reliable authentication methods due to the combination of statistically independent biometric traits [12]. These systems can exploit the benefits of one biometric and mitigate the shortcomings of another biometric. Furthermore, randomly selecting a subset of biometric traits further ensures that the authentic user is presented. The increasing use of multimodal biometrics has led to the investigation of different modes of system operation such as serial mode, parallel mode, and hierarchical mode [11].

III. MULTIMODAL BIOMETRIC-BASED CONTINUOUS USER AUTHENTICATION AND INTRUSION DETECTION

Most authentication systems do not need to re-authenticate the users for continuous access to the protected resources. However, in hostile environments where the chances of a node being captured are high, user authentication is needed not only for the initial login, but also to verify the presence of the authentic user continuously, in order to reduce the vulnerability of the system [9]. The frequency depends on the situation severity and the resource constraints of the network. Using biometrics technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption [3], [11]. Multimodel biometrics can further improve the security performance of the MANETs by utilizing advantages of various biometrics in different situations.

A. MANET with Multi-Modal Biometrics

Multimodel biometrics can further improve the security performance of the MANETs by utilizing advantages of various biometrics in different situations. Biometrics provides a possible solution to authentication in MANETs, because it has a direct connection with the user identity, can be continuously monitored. Multimodel biometric systems present more reliable authentication methods. Combining continuous user authentication and intrusion detection can be an effective approach to improve the security performance in high security MANETs. A single biometric may be inadequate for passive verification either because of noise in the observation samples or because of the unavailability of an observation at a given time. For example, face verification cannot work when frontal face detection fails because the user presents a non frontal pose. To overcome these limitations, researchers have proposed the use of multiple biometrics and have demonstrated increased accuracy of verification with a related decrease in vulnerability to impersonation. The use of multiple biometrics has led to the investigation of integrating different types of inputs (modalities) with different characteristics.

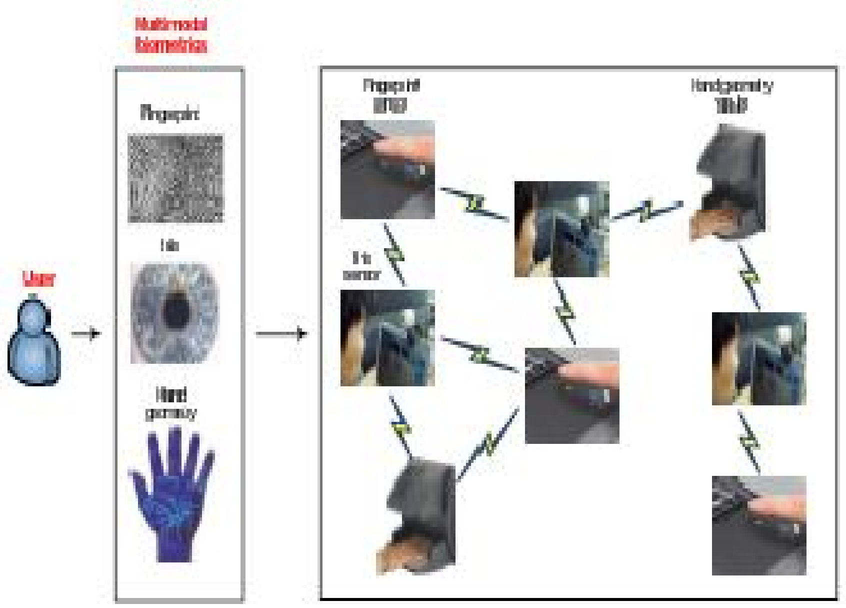

Fig 1. MANET with multimodal biometrics

We use sensor to refer to an authentication device or an intrusion detection device. Without loss of generality, we assume that some nodes have one or more biosensors, and some do not have any biosensor due to the heterogeneity of network nodes in the MANET. Similarly, some nodes are equipped with the IDS, and some are not equipped with the IDS. The total number of network nodes in the MANET is not directly related to the number of sensors.

B. Intrusion Detection Systems and Biometrics

In MANETs, a malicious node can launch deny of service (DOS) or disrupt the routing mechanism by generating error routing messages. For these types of attacks, intrusion detection can serve as a second wall of defense and is of paramount importance in high security networks. An IDS continuously or periodically monitors the current subject activities, compares them with stored normal profiles and/or attack signatures, and initiates proper responses. Two main technologies of identifying intrusion detection in IDSs are 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. The main drawback of misuse detection is that it cannot detect new forms of attacks. Anomaly detection is a behavior-based method, which uses statistical analysis to find changes from baseline behavior. This technology is weaker than misuse detection but has the benefit of catching the attacks without signature existence.

1. Local Data Collection

The local data collection module collects data streams of various information, traffic patterns and attack traces from physical, MAC and network layers via association module. The data streams can include system, user and mobile nodes communication activities within the radio range.

2. Local Detection

The local detection module consists of anomaly detection engine. The local detection module analyzes the local data traces gathered by the local data collection module for evidence of anomalies. A normal profile is an aggregated rule set of multiple training data segments. New and updated detection rules across ad-hoc networks are obtained from normal profile. The normal profile consists of normal behavior patterns that are computed using trace data from a training process where all activities are normal. During testing process, normal and abnormal activities are processed and any deviations from the normal profiles are recorded. The anomaly detection distinguishes normalcy from anomalies as of the deviation data by comparing with the test data profiles with the expected normal profiles. If any detection rules deviate beyond a threshold interval and if it has a very high accuracy rate it can determine independently that the network is under attack and initiates the alert management.

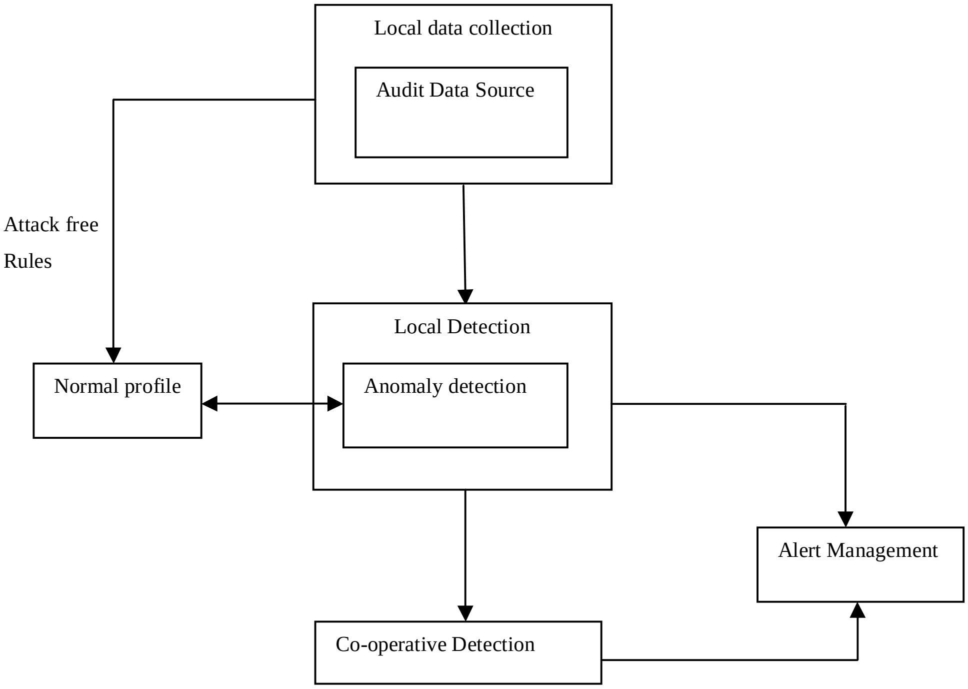

Fig 2. System Architecture for IDS

3. Cooperative Detection

When the support and confidence level is low or intrusion evidence is weak and inconclusive in the detecting node then it can make collaborative decision by gathering intelligence from its surrounding nodes via protected communication channel. The decision of cooperative detection is based on the majority of the voting of the received reports indicating an intrusion or anomaly.

4. Alert Management

The alert management receives the alert from the local detection or co-operative detection depending on the strength of intrusion evidence. It collects them in the alert cache for t seconds. If there are more abnormal predictions than the normal predictions then it is regarded as “abnormal” and with adequate information an alarm is generated to inform that an intrusive activity is in the system.

The partially observable Markov decision process (POMDP) [16] and relevant algorithms can be used solve the combined intrusion detection and continuous authentication problem. Markov model is a very popular approach [10], used in solving security problems. There are several biosensors used for continuous authentication and several sensors used for intrusion detection. Authors of [13] proposed a data pre-processing method to improve a hidden Markov model (HMM) training for host-based anomaly intrusion detection. In this case, both an IDS and an authentication can be run simultaneously. Let $uk \in \{1, . . L\}$ denote the sensor selected at time k, and yk (uk) denote the observation of this sensor. The observations of the lth sensor belong to a finite set of symbols $\{O1(l), O2(l), . . . , OMl\ (l)\}$ and $|Ml|$ denotes the number of possible observations of the lth sensor. When the system state is ei, the lth sensor is picked at time k, the probability of observation m will be obtained from the lth sensor is denoted as: $bi(uk = l, yk = Om(l))$.

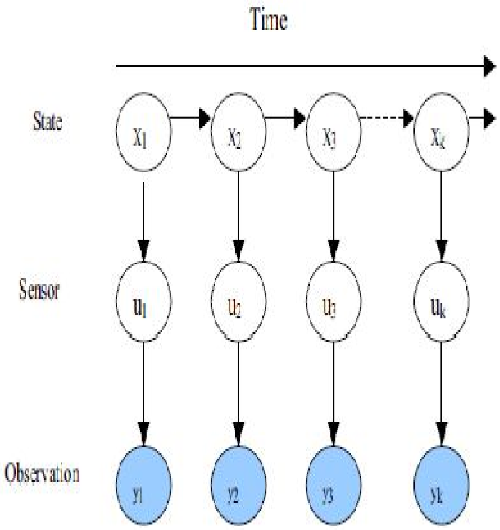

Fig 3. Hidden Markov Model

System procedure can be briefly summarized as three steps,

a. Scheduling: Based on the information state πk, find the optimal sensor uk+1 that will be used at the next horizon.
b. Observation: Observe the output of the optimal sensor yk+1(uk+1) at next horizon.
c. Update: Update the information state πk+1 using the latest observation yk+1.

In biometric authentication and IDS processes, false acceptance (FA) and false negative (FN) errors can result in security breaches, since unauthorized persons are admitted to access the system/network or intrusions are not detected and therefore no alert is raised. The security state of the system may not be observed perfectly due to these errors. Therefore, we formulate the distributed user authentication and intrusion detection scheduling problem as a stochastic partially observed Markov decision process (POMDP) multi-armed bandit problem [14] which is a powerful framework to solve the distributed optimization problem.

C. Gittins Index Policy:

For our proposed scheme, the optimal policy has an index able rule, meaning that the optimal policy can be found according to the Gittins indices of the sensors $(n)(\pi(n)k)(n =1, . . .,N)$ [15]. Optimal policy can be found according to the Gittins indices of the sensors The Gittins index of a sensor is a function of that sensor's characteristics (e.g., state transition probabilities) and its information state. The optimal policy at time is that the sensor with the largest reward Gittins index at that time should be selected. The Gittins index can be monotone increasing in the information state. One common method for computing the Gittins index of each sensor is a value iteration algorithm [10]. In pomdp-solve we chose the incremental pruning algorithm developed in the artificial intelligence, since it one of the fastest algorithms for solving POMDPs [10]. This means that if the information states of these sensors at a given time instant are MLR (Monotone Likelihood Ratio) comparable, the optimal policy is to pick the authentication sensor or the intrusion detection system with the smallest information state with respect to the MLR ordering. The sensor with the higher probability of being in the better state has a higher possibility of being chosen at that time slot.

IV. CONCULSION

Combining continuous user authentication and intrusion detection can be an effective approach to improve the security performance in high security MANETs. In this paper, we presented a distributed scheme of combining user authentication and intrusion detection. In the proposed scheme, the most suitable biosensor (for biometric-based authentication) or IDS is dynamically selected based on the current security posture and energy states in different applications. The problem was formulated as a stochastic multi-armed bandit problem and its optimal policy can be chosen using Gittins indices. We presented a structural result method for calculating the Gittins indices of the sensors in a large network with number of nodes and also reduce the computational complexity.

REFERENCES

[1] S. Mao, S. Kompella, Y. T. Hou, H. D. Sherali, and S. F. Midkiff, "Routing for concurrent video sessions in ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 1, pp. 317–327, Jan. 2006.

[2] T. Sim, S. Zhang, R. Janakriaman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Trans. Pattern Analysis and Machine Intell.*, vol. 29, pp. 687–700, Apr. 2007.

[3] A. Weimerskirch and G. Thonet, "A distributed light-weight authentication model for ad-hoc networks," Lecture Notes in Computer Science, vol. 2288, pp. 341-354, ISBN: 3-540-43319-8, 2001.

[4] K. Ren, W. Lou, K. Kim, and Y. Fang, "A novel privacy preserving authentication and access control scheme for pervasive computing environment," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1373-1384, July 2006.

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

[6] J. Hu, X. Yu, D. Qiu, and H. Chen, "A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection," *IEEE Network*, vol. 23, pp. 42–47, Jan. 2009.

[7] G. A. Jacoby and N. J. Davis, "Mobile host-based intrusion detection and attack identification," *IEEE Wireless Commun.*, vol. 14, pp. 53–60,Aug. 2007.

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

[9] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 8, pp. 806–815, Feb. 2009.

[10] V. Krishnamurthy and B.Wahlberg, "Partially observed Markov decision process multiarmed bandits—structural results," *Math. of Oper. Res.*,vol. 34, pp. 287–302, May 2009.

[11] A. Ross and A. K. Jain, “Multimodal biometrics: an overview,” in *Proc. 12th European Signal Proc. Conf.*, Vienna, Austria, 2004.
[12] A. Ross and A. K. Jain, “Information fusion in biometrics,” *Pattern Recognition Lett.*, vol. 24, pp. 2115-2225, Sept. 2003.
[13] J.C.Gittins, *Multi-Armed Bandit Allocation Indices*. Wiley, 1989.
[14] A. R. Cassandra, “Exact and approximate algorithms for partially observed Markov decision process,” Ph D.dissertation, Brown Univ 1998.