Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Continuous Authentication and Intrusion Detection in Mobile Ad Hoc Network

Varsha S.Upare
Lecturer, Aissms College of Polytechnic

Abstract: *Multimodal biometric technology provides potential solutions for continuous user to device authentication in high security mobile ad hoc networks. Continuous user authentication is an important prevention based approach to protect high security mobile adhoc networks (MANETs). Intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities. This paper presents a framework of combining authentication and intrusion detection in MANET. This paper presents three authentication methods to choose the optimal scheme of combining authentication and intrusion detection.*

1. Introduction

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. This concern is mainly due to the peer-to-peer architecture in MANETs, system resource constraints, shared wireless medium, and highly dynamic network topology [1]. Two complementary classes of approaches exist to protect high security MANETs, prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection [2].

As the front line of defence, user authentication is crucial 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]. For the password, it is simple and easy to use, but difficult to distinguish an authentic user from impostors since there is no direct connection between a user and a password. For the token, in addition to no connection between a user and a token, it is subject to being lost. Biometrics has a direct connection with the identity of the user, and has been studied in MANETs [5]. Multimodal biometrics can be used to alleviate some drawbacks of one mode of biometrics by providing multiple verifications of the same identity [6]. Many efforts have been made to research on either continuous user authentications or hostbased intrusion detection systems. Continuous authentication and intrusion detection can be considered jointly to further improve the performance of high security MANETs. However, little research has been done in combining these two classes of approaches in MANETs.

The authors in [9] proposed a useful framework to combine user authentication and intrusion detection. This paper studies three techniques for combining authentication and intrusion detection in MANETs. Dynamic programming based hidden markov model algorithm used to derive the optimal scheme [9]. The partially observable Markov decision process (POMDP) [10] and relevant algorithms can be used solve the combined intrusion detection and continuous authentication problem. Optimal scheme is chosen based on the information state. The Dumpster–Shafer[7] evidence theory was originated by Dempster and later revised by Shafer. It's essential idea is that an observer can obtain degrees of trust about a proposition from related proposition's subjective probabilities. Multimodal biometrics is combined to work with intrusion detection systems (IDSs) to alleviate the shortcomings of unimodal biometric systems. Since each device in the network has measurement and estimation limitations, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster–Shafer theory for data fusion. Structural result method [8] is used to derive the optimal scheme of combining authentication and intrusion detection in MANET. Fully distributed scheme of combining continuous authentication and intrusion detection in high security MANETs. A user authentication (or IDS) can be scheduled in a distributed manner considering both the security situations and resources (e.g., node energy) in MANETs. The distributed continuous user authentication and intrusion detection scheduling problem is formulated as a POMDP multi-armed bandit problem. Structural results method used for solving the scheduling problem in a large network with a variety of nodes. The rest of this paper is organized as follows. Section 2. Introduces multimodal biometric-based user authentication and intrusion detection in MANETs. Section 3 .Presents

optimal scheme based authentication and intrusion detection. Section 4. Presents Dumpster–Shafer theory for data fusion. Section 5 presents the Structural result method of combining authentication and intrusion detection. Section 6 presents the comparative study of the methods. Section 7. Concludes the paper.

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

2.1 Biometric Authentication:

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. 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 behavioural characteristics. Biometric systems include two kinds of operation models: 1) identification and 2) authentication. 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.

2. 1 IDS:

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 defence 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 [9]. Two main technologies of identifying intrusion detection in IDSs are given as follows: misuse detection and anomaly detection. Misuse detection is the most common signaturebased 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.

3.Optimal Based Authentication and Intrusion Detection

MANET has a continuous authentication system, which is equipped with multiple biosensors and has the ability to collect multiple biometrics, and an IDS, which has the ability to detect intrusions. The time axis is divided into slots of equal duration that corresponds to the time interval between two operations. The length of time slot depends on the security requirements and the system environment. IDS is continuously monitoring the system, the IDS is operated at all time instants. An authentication may be initiated at Second and Following Pagesevery time instant as well. The IDS and authentication may consume extensive system resources, such as battery power, which is an important issue in MANETs. Therefore, it is desirable to optimally schedule intrusion detection and authentication at each time instant taking into account system security requirements and resource constraints. 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. In this case, both an IDS and an authentication can be run simultaneously. Let uk ∈ {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)).

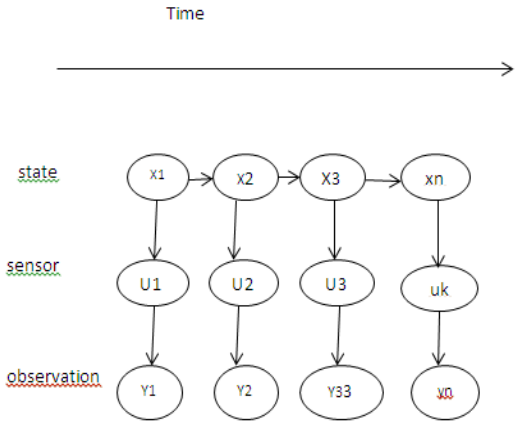

Figure1. Hidden Markov Model

An information state is a sufficient statistic for the history, which means that the optimal sensor (i.e., the optimal operation, intrusion detection or authentication) can be chosen based on the information state, denoted by πk, where k is the time.

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.

3. DATA FUSION OF BIOMETRIC SENSORS AND INTRUSION DETECTION SYSTEM

In the proposed scheme, L sensors are chosen for authentication and intrusion detection at each time slot to observe the security state of the network. To obtain the security state of the network, these observation values are combined, and a decision about the security state of the network is made. However, since there is some probability that a given sensor might either be in a compromised state or have made an inaccurate assessment, it is possible that this sensor has contributed an unreliable observation. It can be quite difficult to ascertain which observers are compromised. Therefore, choosing an appropriate fusion method is critical for the proposed scheme. The decision about which sensors are chosen should not totally depend on the current observation values since the sensors' states are only partially observable. This paper based on the strategy that if the sensors are trustworthy, it always provide accurate observation data. Any chosen node could be untrustworthy due to its current compromised state or inaccurate detection. The chosen node n is trustworthy for an arbitrary observed node a at time slot k + 1 when it is in the secure state and accurately detects. The trustworthy probability tp k+1 (n) of node n at time k + 1 is equal to P(sk+1 n = secure) × P(yk+1 (n) = s k+1 α), where y (n) k+1 is the observation of a's security state obtained from node n. In our scheme, P(y (n) k+1 = secure|s α k+1 = secure) and P(y n k+1 = compromised|sa k+1 = compromised

4.STRUCTURAL RESULTS METHOD FOR COMBINING CONTINUOUS AUTHENTICATION AND INTRUSION DETECTION

The decision about which sensor is chosen at each time slot should depend on all the actions and observations history, since the sensors' states are only partially observable. To this end, information state is developed to derive sufficient statistical information for the past history. 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.

Gittins Index Policy:

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.

Monotone gittins index in the structural results method:

The Gittins index can be monotone increasing in the information state. This means that if the information states of these sensors at a given time instant are MLR 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

COMPARATIVE STUDY

Continuous authentication and intrusion detection improve the performance of high security MANETs. The comparison of three schemes is explained as below.

Table 1. Table example.

Optimal	Structure	Dempster–Shafer theory
Centralized scheme is used. Distributed scheme is used. Distributed scheme used, observation of L sensors are combined.	Centralized scheme is used. Distributed scheme is used. Distributed scheme used, observation of L sensors are combined.	Centralized scheme is used. Distributed scheme is used. Distributed scheme used, observation of L sensors are combined.
Based on the information state, optimal sensor can be picked. Optimal policy can be found by gittins index rule. Based on the giitins index , optimal sensor is used.	Based on the information state, optimal sensor can be picked. Optimal policy can be found by gittins index rule. Based on the giitins index , optimal sensor is used.	Based on the information state, optimal sensor can be picked. Optimal policy can be found by gittins index rule. Based on the giitins index , optimal sensor is used.
Computational complexity is	Computational complexity is	Computationa l complexity

more. Computational complexity is reduced in Structural result. Computational complexity is reduced.	more. Computational complexity is reduced in Structural result. Computational complexity is reduced.	is more. Computational complexity is reduced in Structural result. Computational complexity is reduced.
Centralized scheme overhead is 8+4N bytes per slot. Total communication overhead is 8*(N-1) bytes per time slot. Total communication overhead is 8*(N- 1)bytes per slot.	Centralized scheme overhead is 8+4N bytes per slot. Total communication overhead is 8*(N-1) bytes per time slot. Total communication overhead is 8*(N- 1)bytes per slot.	Centralized scheme overhead is 8+4N bytes per slot. Total communication overhead is 8*(N-1) bytes per time slot. Total communication overhead is 8*(N- 1)bytes per slot.
In the centralized scheme incremental pruning algorithm is used. In the distributed scheme, structural result method is used. In this Dumpster–Shafer theory used for data fusion.	In the centralized scheme incremental pruning algorithm is used. In the distributed scheme, structural result method is used. In this Dumpster–Shafer theory used for data fusion.	In the centralized scheme incremental pruning algorithm is used. In the distributed scheme, structural result method is used. In this Dumpster–Shafer theory used for data fusion.
Used for small no of nodes. Used for large number of distributed nodes. Used for larger number of distributed nodes.	Used for small no of nodes. Used for large number of distributed nodes. Used for larger number of distributed nodes.	Used for small no of nodes. Used for large number of distributed nodes. Used for larger number of distributed nodes.
Two security states and two energy are considered. Three security and three energy states are considered.	Two security states and two energy are considered. Three security and three energy states are considered. Two	Two security states and two energy are considered. Three security and three energy states are
Two security and two energy states are considered	security and two energy states are considered	considered. Two security and two energy states are considered

CONCLUSION

Continuous authentication and intrusion detection jointly improve the security performance of the Manet. This paper, presented a distributed scheme combining authentication and intrusion detection. Dempster–Shafer theory has been used for IDS and sensor fusion since more than one device is used at each time slot. The distributed multimodal biometrics and IDS scheduling process can be divided into offline and online parts. In the structural result method , the optimal policy can be chosen based on the gittins index. Structural results method used for calculating the Gittins indices of the sensors in a large network with a variety of distributed nodes. Intrusion detection is modelled as noisy sensors that can detect the system security state (safe or compromised). Continuous authentication is performed with multimodal biometrics.This paper presents the comparative study of different techniques which is used to combine authentication and intrusion detection.

4. References.

[1] Briand, L. C., Daly, J., and Wüst, J., "A unified framework for coupling measurement in objectoriented systems", *IEEE Transactions on Software Engineering*, 25, 1, January 1999, pp. 91-121.

[2] Maletic, J. I., Collard, M. L., and Marcus, A., "Source Code Files as Structured Documents", in *Proceedings 10th IEEE International Workshop on Program Comprehension (IWPC'02)*, Paris, France, June 27-29 2002, pp. 289-292.

[3] A. Weimerskirch and G. Thonet, "A distributed lightweight 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] Salton, G., *Automatic Text Processing: The Transformation, Analysis and Retrieval of Information by Computer*, Addison-Wesley, 1989.

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

[7] S. Bu,F.yu,X.Liu, P. Mason, and H. Tang,"Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks,"in IEEE Trans, vehicular technology, vol. 60, no. 3, march 2011.

[8]S.Bu. F. Yu, P. Liu,"Structural Results for Combined Continuous UserAuthentication and IntrusionDetection in High Security Mobile Ad-Hoc Networks,"IEEE Wireless Commun, vol. 10, no. 9, Sep 2011.

[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] A. R. Cassandra, "Exact and approximate algorithms for partially observed Markov decision process," Ph D.dissertation, Brown Univ 1998.