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. 3, Issue 6, June 2015

Highly Secured Authentication and Authorization Using Partially Observable Markov Decision Process in MANETs

N. Rajesh [1],K. Madhavan [2], R. Vinoth [3]

Assistant Professor, Dept. of CSE, Chennai Institute of Technology, Chennai, Tamilnadu, India [1]

Assistant Professor, Dept. of CSE, Chennai Institute of Technology, Chennai, Tamilnadu, India[2]

Sap Basis Team, Kaar Technologies, Chennai, Tamilnadu, India[3]

ABSTRACT*:* Continuous user authentication is an important prevention-based approach to protect high security mobile adhoc networks (MANETs). Intrusion detection systems (IDSs) are also significant in MANETs to identify malicious activities. Considering these two approaches mutually is an effective in optimal security design to protect high security MANETs. User authentication and authorization desires to be performed continuously and frequently, since the chance of a device in a hostile environment being captured is extremely high. To obtain the optimal scheme of combining continuous authentication and IDSs in a distributed manner, we formulate the scheduling problem as a Partially Observable Markov Decision Process (POMDP) multi-armed bandit problem. We present optimal Gittins index policy to solve the scheduling problem for a huge network. The Gittins index of a process is a function of that process's characteristics and its information state. Value iteration algorithm is used for computing Gittins index. For each process, information state and Gittins rewards are calculated. Based on the information states and the rewards, the processes are scheduled using POMDP policies. The optimal policy is to select the process with the largest reward Gittins index. The process with the higher probability of being in the better state has a higher possibility of being chosen at that time slot. The optimal policy picks the authentication process or the intrusion detection system with the largest Gittins rewards.

KEYWORDS: Biometric traits, Continuous authentication, intrusion detection system, mobile adhoc network, POMDP.

I. Introduction

In MANETs (Mobile Adhoc Networks), security is most important one when communication takes place. Authentication is one of the security service which is a process of confirming the correctness of the claimed identity. In MANET, to provide high authentication and authorization security, the prevention-based (such as user authentication) and detection-based (such as intrusion detection system) are combined in many applications.

Authentication deals with whether you are actually communicating with a particular entity. Authentication is a prevention based approach. User authentication can be performed by using one or more types of validation factors: Knowledge factors (such as passwords), possession factors (such as tokens) and biometrics technology. Knowledge factors and possession factors can make it difficult to distinguish an authenticated user from an imposter if there is no direct connection between a user and a password or a token. Biometrics technology provides direct connection between a user and their identity. User authentication wants to be performed frequently and continuously. Using Biometric technology, individuals can be automatically and continuously identified and verified by their physiological or behavioral characteristics without user interruption.

Common physiological traits include fingerprints, iris, hand geometry, retina and facial images. The behavioral biometric traits includes signature, voice recordings. Biometric technology provides possible solutions to the continuous user authentication problem for MANETs[8], as it has direct communication with user identity. Intrusion

DOI: 10.15680/ijircce.2015.0306142

detection is also essential to effectively identify the malicious activities. IDSs can be categorized as follows[17]: 1) Router based intrusion detection, which is installed on the routers to prevent intruders; 2) Network-based intrusion detection, which runs at the gateway of the network and examines all incoming packets;3) host-based intrusion detection, which receives the audit data from the host operating system and analyzes the generated events to keep local node secure. For the MANETs, host-based IDSs are suitable as no centralized gateway or route exists in the network[7].

Continuous authentication and intrusion detection system are considered jointly to improve the performance of high security MANETs. Many efforts have been done for combining these two approaches in MANETs. Authors in[3] proposed a centralized scheme to combine user authentication and intrusion detection. In this proposed centralized scheme[3], the whole system formulated as a single partially observable markov decision process (POMDP). Solving POMDP can be intractable as the state space of the POMDP increases with the number of biometric sensors and IDSs[10].

In this paper, we combine both continuous authentication and intrusion detection in a fully distributed manner for high security MANETs. A user authentication and intrusion detection can be scheduled in a distributed manner considering both the security situations and resources. The continuous user authentication and intrusion detection scheduling problem is formulated as a POMDP multi-armed bandit problem. The optimal gittins index policy using value iteration algorithm has been chosen to solve the scheduling problem in a huge network with variety of nodes. The results are derived to show the performance of the proposed scheme.

The rest of the paper is structured as follows: Section II describes a short review of the related work. Section III introduces the proposed scheme for continuous authentication and intrusion detection. The experimental results were presented in Section IV. Finally, Section V describes the concluding remarks and suggestions for future work.

II. RELATED WORK

Most authentication system do not need to re-authenticate the users for continuous access to the confined resources. 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.

Shengrong Bu, et al.[1] proposed structural results method for solving the scheduling problem in a large network. In this system, the most suitable biosensor or IDS is dynamically selected based on the current security posture and energy states. Scheduling problem formulated as partially observable markov decision process(POMDP) multi-armed bandit problem. The optimal policy was derived to schedule the optimal sensors. The optimal policies were derived from structural results and scheduled both biometric sensors and intrusion detection system.

Shengrong Bu at al.[2] proposed data fusion method. Multimodal biometrics are deployed to work with intrusion detection systems. This system decides whether user authentication is mandatory and which bio sensors should be chosen. The decisions were made by each authentication device and IDS. More than one biosensor and IDS is chosen to detect the security states of the system. More than one device needed to be chosen and observations can be fused to increase observation accuracy. In the proposed scheme, the most suitable biosensors for authentication or IDSs were dynamically chosen based on security posture and energy states. Dempster-Shafer theory has been used for biosensor and IDS fusion since more than one device is used at each time slot.

J. Liu at al.[3] proposed a framework in which whole system is formulated as a Partially Observed Markov Decision Process considering both security requirements and resource constraints. Dynamic programming based Hidden Markov Model Scheduling Algorithms have been employed to derive the optimal schemes for both intrusion detection and continuous authentication. In this approach, distinct features are as follows, it can optimally control whether or not to perform an authentication as well as which biometrics to use to minimize the usage of the system resources, decides that whether or not to activate IDS, system security requirement constraints and resource constraints can be guaranteed. The whole system is formulated as a partially observable markov decision process (POMDP). In this formulation,

DOI: 10.15680/ijircce.2015.0306142

continuous authentication and intrusion detection system can share history information with each other. The optimal policy can be acquired by solving POMDP with dynamic programming-based hidden makov model scheduling algorithms.

Vikram Krishnamurthy at al.[4] proposed a framework in which Optimal sensor scheduling problem is formulated as a partially observed Markov decision process. This system computes the optimal measurement scheduling policy which has threshold structure with respect to a monotone likelihood ratio ordering.

Jiankun Hu at al.[5] proposed a framework in which a host-based anomaly IDS is an effective complement to the network IDS in addressing issue. This article proposes a simple data preprocessing approach to speed up a Hidden Markov Model (HMM) training for system-call-based anomaly intrusion detection.

Jie Liu at al.[6] proposed a framework in which multimodal biometrics are used for continuous authentication and intrusion detection is modeled as sensors to detect system security state. This system used dynamic programming based algorithms to derive the optimal schemes for both intrusion detection and continuous authentication. Multimodal biometrics is used for continuous authentication and intrusion detection is modeled as sensors to detect system security state. This system used dynamic programming based algorithms to derive the optimal schemes for both intrusion detection and continuous authentication. This proposed scheme is a centralized scheme in which the whole system formulated as a single partially observable markov decision process (POMDP).

III. PROPOSED ALGORITHM

Continuous Authentication is to verify the presence of an authentic user. User authentication is needed to be done frequently and continuously in order to reduce vulnerability of a system. The frequency depends on the situation severity of the system. Multimodal biometrics can improve the security performance of the MANETs. Mobile adhoc network can be equipped with Bio-sensors and intrusion detection system. Some nodes can be equipped with one or more bio-sensors and some do not have any biosensors. Similarly, some nodes can be equipped with IDS, and some do not have IDS.

The system can perform two types of operations: user authentication and intrusion detection. User authentication can be executed at every time instant and intrusion detection system can operate to monitor the system at all time instants. It is critical for the system to schedule the intrusion detection and user authentication continuously in a distributed manner. The conventional biometric authentication and intrusion detection system can be resulted in false acceptance and false negative errors, since sometimes unauthorized persons are admitted to access the system. Thus, malicious activities are not properly detected for secured communication. Therefore, the user authentication and intrusion detection scheduling problem as a stochastic Partially Observed Markov Decision Process (POMDP) multi-armed bandit problem[10]. The optimal Gittin’s index policy solves the scheduling problem using value iteration algorithm.

A. System Model

Here, the time axis is divided into equal time slots, which corresponds to the time intervals between continuous authentication and intrusion detection system. Let the state of a sensor n, n {1,2,….,N}, the security condition of each sensor can be divided into L discrete

DOI: 10.15680/ijircce.2015.0306142

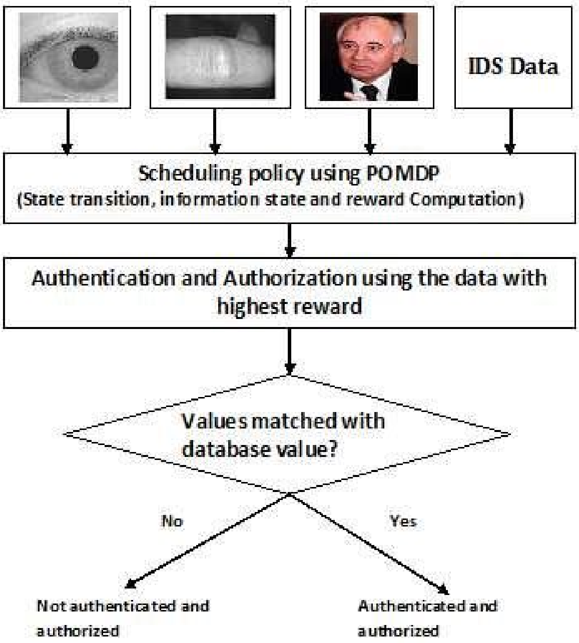
IDS Data
Scheduling policy using POMDP
(State transition, information state and reward Computation)
Authentication and Authorization using the data with highest reward
Values matched with database value?
No
Yes
Not authenticated and authorized
Authenticated and authorized

Fig.1. Architecture Diagram

levels, such as{secured, attacked, compromised}. The security state space involves all the security states{s1,….s_L}. if sensor p is idle at time k, the state of this idle sensor is unchanged.

In MANETs, the state of the chosen sensor p may not be observed directly. The observation of its state includes the observation of its security state. The decision about which sensor is chosen at each time slot should depend on all actions and observation history, since the state of the sensor are only partially observable. The information state is developed to derive statistical information for the past history. The information state of the sensor refers to the probability distribution over the sensors states. The optimal sensor can be chosen based on the information state[9].This optimal policy picks the authentication system or intrusion detection system with the smallest information state.

B. Gittin's Index Policy

Optimal policy is to select the biometric data with largest reward Gittins index at a particular time instant, where the Gittins index of each process is a function of the state of that process only. Value iteration algorithm is used for computing Gittins index.

(i) State Transition Probability Matrix:

Consider P independent projects, enumerated by p = 1,….P. Each project p has a finite number of states N_p. Let $s_k^{(p)}$ denote the state of project p at discrete time k = 0,1,…..

At each time instant k only one of these projects can be worked on. The state $s_k^{(p)}$ evolves according to an N_p state homogeneous Markov chain with transition probability matrix,

$A^{(p)}=(a_{ij}^{(p)})=P(s_{k\ |1}^{(p)}=j \mid s_k^{(p)}=i)$ (1)

Where i , j N$|p$

(ii) Observation Probability Matrix:

The state of the active project p is indirectly observed

via noisy measurements (observations) $y_{k\ 1\ |}^{(p)}$ of the | |

active project state $s_{k\ 1}^{(p)}$. These observations $y_{k\ 1}^{(p)}$ belong to a finite set Mp indexed by $m_{(p)}$= 1,…..,Mp. Let $B^{(p)}=(b_{im}^{(p)})$ i N$|$ p ; |

m Mp denote the observation probability (symbol probability) matrix of the Hidden Markov Model (HMM), the observation probability matrix,

$B^{(p)}=(b_{im}^{(p)})$, m M$|p$ and i N$|p$ where

$b_{im}^{(p)}=P(y_{k\ |1}^{(p)}=m \mid s_{k|\ 1}^{(p)}=I;\ u_k=p)$

(iii) Information State Calculation

Information state refers to probability distribution over project’s states. The optimal project is chosen based on the information state. For each project p, the information

state, denote by x_k

$x_{k\ (p)}=(x_k^{(p)}(i))\ i=1,\ldots\ldots,\ N_p$ (2)

where $x_k^{(p)}(i)=P(s_{k\ 1|}^{(p)}=j \mid Y_k\ \ U_{k\text{-}1})$

(iv) Reward Function Calculation

Let $u_k=\{1\ldots\ldots,P\}$ denote which project is worked on

at time k. Consequently, $s_{k\ 1|}^{(u_k)}$ denotes the state of the active project at time k + 1. Let the policy denote the stationary sequence of controls, $\{u_k, k=1,2\ldots\ldots\}$. The

total expected discounted reward over an infinite time horizon is given by,

$$J_i = E\left[\sum_{k}^{\infty}\beta^{k} R(s_{k\ 1} \mid {}^{(u_k)}, u_k \right] \qquad (3)$$

Where β is a discount factor and E denotes mathematical expectation. The aim is to determine the optimal stationary policy which yields the maximum reward in (1).

(v) Gittins Index Computation

It is well known that the optimal policy has an indexable rule. For each project p there is a function $\gamma^{(p)}(x^{(p)})$called the Gittins index, which is only a function of

the project p and the information state $x_k^{(p)}$, whereby the

optimal scheduling policy at time k is to work on the project with the largest Gittins index, i.e., choose project q, where q =

arg max p $\{1.,\ldots,P\}$ $(\gamma^{(p)}\ (x^{(p)}))$. Thus computing the

Gittins index is a key requirement for solving any multi-armed bandit problem.

(vi) Value Iteration Algorithm for computing gittins index:

This section presents a value iteration algorithm for computing Gittins index $\gamma^{(p)}(x^{(p)})$ for each project

$p \quad \{1,\ldots..,P\}$

$$\gamma_N^{(p)}(x^{(p)}) = \mathrm{Min}\{ M: V^{(p)}(x^{(p)}, M) = M\} \quad (4)$$

where

$$V^{(p)}(x^{(p)}, M) = \max\{ R`(p)\, x^{(p)} + \beta \sum_{m=1}^{M_p} \left( V^{(p)}\left(\frac{B^{(p)}(m)A^{(p)}`x^{(p)}}{1`N_p B^{(p)}(m)A^{(p)}`x^{(p)}}, M\right) 1`N_p B^{(p)}(m)A^{(p)}`x^{(p)}, M \right\} \qquad (5)$$

(vii) Optimal Policy Computation

The optimal policy at time k is that the project with largest reward Gittins index at that time should be selected when the reward is the optimization objective, which significantly decreases the computational complexity.

$$\mu^{*} = \arg\max \mid U\ J_{\mu} \qquad (6)$$

where U denotes the set of sequences u k which map Y_k to

{1,……,P}

IV. EXPERIMENTAL RESULTS

In this section, the proposed distributed scheme results are given. The proposed scheme schedules the sensors data dynamically to provide continuous authentication. We consider the following scenario. There are three types of data for continuous authentication, iris data, finger knuckle data and face data, and IDSs for intrusion detection. Each data has five states (more secure, secure, safe, compromised, attacked). The iris, finger knuckle, face data provides the most accurate authentication. IDS monitors the system at all time instants and provides security state of the system.

Initially each process start with secure state of the all data.

Given below TABLE 1 Iris, finger knuckle, face and IDS sensors' data are given as input. For a given input data, the state transition probabilities, information state and reward function values are computed for a given input. The gittin's index policy is applied to select one
Given below TABLE 2 for the given value for Iris, finger the result reward value is computed.

biometric data or IDS for continuous authentication and authorization.

TABLE I

Security State information of Iris and Finger Knuckle

Data	Range of key values	Matching score	Security state	Authentication result
Iris	22.00 – 29.55	Above 80%	1(safe)	Valid
Finger knuckle	61.00-69.00	Above 80%	1(safe)	Valid
Iris	22.00 – 29.55	Above 50%	2(compromised)	Valid
Finger knuckle	61.00-69.00	Above 50%	2(compromised)	Valid
Iris	22.00 – 29.55	Below 50%	0(attacked)	Invalid
Finger knuckle	61.00-69.00	below 50%	0(attacked)	Invalid

TABLE II

Continuous Authentication Results

Input data	Reward value
Iris , Finger knuckle	1.600000023841858, 0.800000011920929
Iris , Finger knuckle	1.600000023841858, 0.800000011920929
Iris , Finger knuckle	1.600000023841858, 0.800000011920929

A. Computational Efficiency

In the centralized scheme [3], the whole network is formulated as a single POMDP and a centralized controller required to schedule the authentication and intrusion detection. Since the state space of the POMDP grows exponentially with the number of sensors to be scheduled. By contrast, in the proposed scheme, the optimal policy schedules individual sensors by Gittin's index. Therefore, the computational complexity of the proposed scheme is considerably decreased. From Table I and II, iris and finger knuckle data have been taken as input and applied scheduling policy, and the results are given only for iris and finger knuckle data.

B. Performance Comparison

The proposed scheme provides optimal policies that minimizes the information leakage, since it is a distributed scheme in which the information is not shared among nodes. Fig. 2 shows that the information leakage is smaller when the system becomes more secure. High transition probability means that the system is more secure.

C. Network Lifetime Comparison

The proposed scheme increases the network lifetime, since instead of performing re-authentication, the

proposed system performs continuous authentication. In existing system, one or more biometric data has been chosen for continuous authentication and authorization.

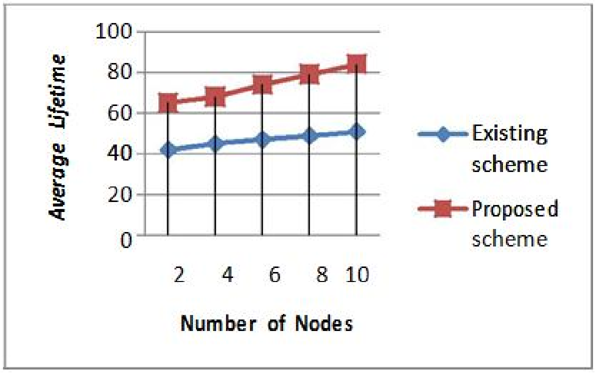

Fig.2. Network average life time with varying number of nodes.

In proposed system, only one biometric trait is going to be selected and Continuous authentication is done in a

DOI: 10.15680/ijircce.2015.0306142

distributed manner. Network lifetime has been increased as the proposed system reduces the computational complexity.

The optimal scheduling policy schedules the given input data and provides the results for continuous authentication. Table I provides the security state information of the iris and finger knuckle data. Fig.2 illustrates network average life time with varying number of nodes.

V. Conclusion and Future Work

Combining continuous 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 system. In the proposed scheme, the most suitable biometric data or IDS is dynamically selected based on the current security state. The scheduling problem was formulated as a stochastic multi-armed bandit problem, and an optimal policy can be chosen using Gittins indices. Value iteration algorithm is presented for calculating Gittins indices of sensors in large network with a variety of distributed nodes. Results are presented using value iteration algorithm with lower computational complexity. The proposed scheme decreases the computational complexity and increases the network lifetime. Future work is in progress to consider face biometric trait and other biometric traits such as palm print in making the scheduling decisions and also to increase the network life time in MANETs.

References

1.Shengrong Bu, F. Richard Yu, Xiaoping P. Liu and Helen Tang, ―Structural Results for Combined Authentication and Intrusion Detection in High Security Mobile Adhoc Networks,‖ IEEE Trans. On Wireless Communications., vol. 10, no. 9, pp. 3064-3073, Sep 2011.

2.Shengrong Bu, F.Richard Yu and Helen Tang, ‖Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad hoc Networks‖, IEEE Trans., Vol. 60, No.3, MAR 2011.

3.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.

4.V. Krishnamurthy and D. Djonin, ―Structured threshold policies for dynamic sensor scheduling—a partially observed Markov decision process approach,‖ IEEE Trans. Signal Process., vol. 55, no. 10, pp. 5069–5083, Oct. 2007.

5.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.

6.Jie Liu, F. Richard Yu and Chung-Horng Lung, ―A framework of combining Intrusion Detection and Continuous Authentication in Mobile Ad Hoc Networks,‖ IEEE Trans. Wireless Commun., Vol. 8, No. 2, pp. 806-815, Feb 2008.

7.A. Mishra, K. Nadkarni, and A. Patcha, ―Intrusion detection in wireless ad-hoc networks,‖ IEEE Wireless Commun., vol. 11, pp. 48–60, Feb 2004.

8.Q. Xiao, ―A biometric authentication approach for high security ad-hoc networks,‖ in Proc. IEEE Info. Assurance Workshop, June 2004.

9.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.

10.V. Krishnamurthy and B.Wahlberg, ―Partially observed Markov decision process multi-armed bandits—structural results,‖ Math. of Oper. Res., vol. 34, pp. 287–302, May 2009.

11.V. Krishnamurthy and D. Djonin, ―Structured threshold policies for dynamic sensor scheduling—a partially observed Markov decision process approach,‖ IEEE Trans. Signal Process., vol. 55, no. 10, pp. 5069– 5083, Oct. 2007.

12.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.

13.J.Megiba and A.Vijayakumar ,‖Fusion Based Multimodal Biometric Authentication with Anamoly Intrusion Detection System‖, Internatioanal conference in Megna On Emerging Engineering Trends., pp. 216-221, Apr 2012.

14.J. Koreman, 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.

15.V. Krishnamurthy and B. Wahlberg, ―Partially observed Markov decision process multiarmed bandits—Structural results,‖ Math. Oper. Res., vol. 34, no. 2, pp. 287–302, May 2009.

16.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.

17.S. K. Das, A. Agah, and K. Basu, ―Security in wireless mobile and sensor networks,‖ in Wireless Communications Systems and Networks. New York: Plenum, Jan. 2004, pp. 531–557.

18.V. Krishnamurthy, ―Algorithms for optimal scheduling and management of hidden Markov model sensors,‖ IEEE Trans. Signal Process., vol. 50,no. 6, pp. 1382–1397, Jun. 2002.

19.T. M. Chen and V. Venkataramanan, ―Dempster-Shafer theory for intrusion detection in ad hoc networks,‖ IEEE Internet Comput., vol. 9, no. 6, pp. 35–41, Nov. 2005.