Middle-East Journal of Scientific Research 19 (7): 904-907, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.19.7.1467

Authentication and Authorization for High Security Manets

D. Kerana Hanirex and K.P. Kaliyamurthie

Bharath University, Chennai-73, India

Abstract: User authentication is an important prevention-based approach to protect mobile adhoc networks (MANETs). Intrusion detection systems (IDSs) are also important in MANETs to identify malicious activities. Biometric technology provides some possible solutions to the continuous user authentication problem in MANETs, since it has direct communication with user identity. Intrusion detection is also important to effectively identify the malicious activities. we develop the scheduling problem as a partially observable Markov decision process (POMDP) multi-armed bandit problem. We present optimal Gittins index policy to solve the problem for a large network.

Key words: Continuous authentication · Intrusion detection system · Optimal scheduling policy

INTRODUCTION

Biometric technology refers to any technique that uses measurable physiological or behavioral characteristics that distinguish one person from another [1]. Using Biometric technology, individuals can be automatically and continuously identified and verified by their physiological and behavioral characteristics without user interruption. Common physiological traits include fingerprints, hand geometry, retina, iris and facial images. The behavioral biometric traits includes signature, voice recordings. Biometric authentication is sufficient to identify the authorized person. Continuous authentication is to verify the presence of authentic user in order to reduce vulnerability of a system. Continuous authentication is performed by scheduling all the biometrics in order to increase the network life time [2-6].

Intrusion Detection Systems continuously or periodically monitors the current subject activities. Intrusion detection systems are important to identify malicious activities. IDS can be categorized as network based intrusion detection which runs at the gateway of the network and examines all the incoming packets, router based intrusion detection which is installed on the routers to prevent the intruders from entering the network, host based intrusion detection which receives the necessary audit data from host's operating system and analyzes the generated events to keep the local node secure. For mobile adhoc networks (MANETs), host based IDS s are suitable [7-10].

Scheduling problem is formulated as partially observed markov decision process (POMDP) problem. The optimal policies for scheduling are derived to solve the POMDP problems using many algorithms. The optimal policies are to select the any one of operations with highest reward of Gittins index which is more appropriate policy for decision making. Gittin index of a particular process is a function of that process's characteristics (state transition probabilities) and it's information state.

Markov Decision Process is a markov chain in which state transitions depend on the current state.Partially Observable Markov Decision Process is a markov decision process in which state of the system is only partially observable. The optimal policies are derived to solve POMDP problems [11].

Previous Research: In the previous work, whole system is formulated as a Partially Observed Markov Decision Process considering both security requirements and resource constraints. This approach, can optimally control an authentication as well as which biometrics to use to minimize the usage of the system resources. System security requirement constraints and resource constraints can be guaranteed. This system used

Corresoponding Author: D. Kerana Hanirex, Bharath University, Chennai-73, India.

Dynamic programming based algorithms to derive the optimal schemes for both intrusion detection and continuous authentication.

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. In this paper, Multimodal biometrics are deployed to work with intrusion detection system. This system decides whether user authentication is required and which bio sensors should be chosen [12]. The decisions are 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 needs to be chosen and observations can be fused to increase observation accuracy.

J. Liu, F. 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, No. 2, pp. 806-815, Feb 2009. In this paper, the proposed scheme is a centralized scheme in which the whole system is formulated as a single partially observable markov decision process. In this work, it is assumed that authentication decisions should be based solely on the outcome from the authentication systems and intrusion detection should be based on a different set of information. In this work, the whole system is formulated as a partially observable markov decision process(POMDP). The optimal policy can be acquired by solving POMDP with dynamic programming based hidden markov model(HMM) scheduling algorithmsIn this work, 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. System security requirement constraints and resource constraints can be guaranteed.

Vikram Krishnamurthy and Dejan V. Djonin," Structured Threshold Policies for Dynamic Sensor Scheduling-A Partially Observed Markov Decision Process Approach," *IEEE Trans on Signal Processing*, Vol. 55, No. 10, Oct 2007. In this paper, 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 and Xinghuo Yu and Hsiao-Hwa Chen," A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection" In this paper, A host-based anomaly IDS is an effective complement to the network IDS in addressing this issue. This paperproposes a simple data preprocessing approach to speed up a hidden Markov model (HMM) training for system-call-based anomaly intrusion detection.

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. In this paper, 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.

Hypotheses:

H1: Information state calculation
H2: Reward function
H3: Gittins index computation
H4: Optimal policy.

MATERIALS AND METHODS

In this system, an optimal scheduling scheme is proposed for making decision to choose one biometric data or IDS. Security issue is an important issue for mobile adhoc networks. Two classes of approach, prevention-based(user authentication) and detection-based (Intrusion detection system) can be used to protect high security MANETs. Biometric technology refers to any technique that uses measurable physiological or behavioral characteristics that distinguish one person from another. Using Biometric technology, individuals can be automatically and continuously identified and verified by their physiological and behavioral characteristics without user interruption. Common physiological techniques include fingerprints, hand geometry, retina, iris and facial images. The behavioral biometric traits includes signature, voice recordings. Biometric authentication is sufficient to identify the authorized person. Continuous authentication is to verify the presence of authentic user in order to reduce vulnerability of a system. Continuous authentication is performed by scheduling all the biometrics in order to increase the network life time.

Intrusion Detection Systems continuously or periodically monitors the current subject activities [13]. Intrusion detection system involves detecting patterns of activity that are known to correlate with intrusions. Intrusion detection systems are important to identify malicious activities. IDS can be categorized as network based intrusion detection which runs at the gateway of the network and examines all the incoming packets, router based intrusion detection which is installed on the routers to prevent the intruders from entering the network, host based intrusion detection which receives the necessary audit data from host's operating system and analyzes the generated events to keep the local node secure. Continuous user authentication and intrusion detection can be combined to improve the performance of high security MANETs. Continuous authentication is to verify the presence of an authentic use and IDS continuously and periodically monitors the subject activities and compares them with stored normal profiles and/or attack signatures and initiates proper responses. User authentication needs to be done continuously and frequently. It is critical to schedule the intrusion detection and authentication activities for each time slot, taking system security and resource constraint into account. Scheduling problem is formulated as a partially observable markov decision process(POMDP) multi-armed bandit problem. The optimal Gittin's index scheduling policy is derived to solve scheduling problem using value iteration algorithm [14].

This paper proposes an optimal policy for decision making process using POMDP. In this paper, one biometric data are used, iris data to improve the security and intrusion detection system is used to detect the system security state. User authentication needs to be performed continuously and frequently, since the chance of a device in a hostile environment being captured is extremely high. Based on the security state of the network, biometric data and intrusion detection system is scheduled and either biometrics data or intrusion detection system is chosen for continuous authentication and authorization in order to reduce the vulnerability of a system.

CONCLUSION

Combining continuous authentication and intrusion detection is an efficient 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 biosensor or IDS is dynamically selected based on the current security state. The problem was formulated as a stochastic multi-armed bandit problem and an optimal policy can be chosen using gittins indices. Future work is to consider more nodes' states in making the scheduling decisions in MANETs and also to increase the network life time [15-17].

REFERENCES

1. Xiao, Q., 2004. A biometric authentication approach for high security ad-hoc networks, in Proc. IEEE Info. Assurance Workshop.
2. Mishra, A., K. Nadkarni and A. Patcha, 2004. Intrusion detection in wireless ad-hoc networks," IEEE Wireless Commun., 11: 48-60.
3. Sim, T., S. Zhang, R. Janakriaman and S. Kumar, 2007. Continuous verification using multimodal biometrics, IEEE Trans. Pattern Analysis and Machine Intell., 29: 687-700.
4. Krishnamurthy, V. and D. Djonin, 2007. Structured threshold policies for dynamic sensor scheduling-a partially observed Markov decision process approach, IEEE Trans. Signal Process., 55(10): 5069-5083.
5. Jie Liu, F. Richard Yu and Chung-Horng Lung, 2008. A framework of combining Intrusion Detection and Continuous Authentication in Mobile Ad Hoc Networks, IEEE Trans. Wireless Commun., 8(2): 806-815.
6. Hu, J., X. Yu, D. Qiu and H. Chen, 2009. A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection, IEEE Network, 23: 42-47.
7. Jacoby, G.A. and N.J. Davis, 2007. Mobile host-based intrusion detection and attack identification, IEEE Wireless Commun., 14: 53-60.
8. Krishnamurthy, V. and D. Djonin, 2007. Structured threshold policies for dynamic sensor scheduling-a partially observed Markov decision process approach, IEEE Trans. Signal Process., 55(10): 5069-5083.
9. Liu, J., F.R. Yu, C.H. Lung and H. Tang, 2009. Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks, IEEE Trans. Wireless Commun., 8: 806-815.

10. Varsha, S. Upare and Lalit Kulkarni, 2013. Multimodal Biometric Authentication and Intrusion Detection in Mobile Ad Hoc Network, JGRCS, 4(1).
11. Kumaravel, B. Anatha Barathi, 2013. Personalized image search using query expansion, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 15(12): 1736-1739.
12. Kumaravel, A. and R. Udayakumar, 2013. Web Portal Visits Patterns Predicted by Intuitionistic Fuzzy Approach, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4549-4553.
13. Kumaravel, A. and K. Rangarajan, 2013. Algorithm for Automation Specification for Exploring Dynamic Labyrinths, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4554-4559.
14. Kumaravel, A. and Oinam Nickson Meetei, 2013. An Application of Non-uniform Cellular Automata for Efficient Crytography, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4560-4566.
15. Pattanayak, Monalisa and P.L. Nayak, 2013. Green Synthesis of Gold Nanoparticles Using Elettaria cardamomum (ELAICHI) Aqueous Extract World Journal of Nano Science & Technology, 2(1): 01-05.
16. Chahataray, Rajashree. and P.L. Nayak, 2013. Synthesis and Characterization of Conducting Polymers Multi Walled Carbon Nanotube-Chitosan Composites Coupled with Poly (P-Aminophenol) World Journal of Nano Science & Technology, 2(1): 18-25.
17. Parida, Umesh Kumar, S.K. Biswal, P.L. Nayak and B.K. Bindhani, 2013. Gold Nano Particles for Biomedical Applications World Journal of Nano Science & Technology, 2(1): 47-57.