ISSN:0975-9646

Dynamic Intrusion Detection with Data Fusion and Aggregation in High-Security Mobile Ad Hoc Networks

*T.Kumanan,**Dr.K. Duraiswamy

**Meenkashi College of Engineering, K.K.Nagar, Chennai – 78.*
***K.S.R. College of Technology, Thiruchengodu, Tamil Nadu.*

Abstract—Multimodal biometric technology provides potential solutions for continuous user to device authentication in high-security mobile ad hoc networks (MANETs). This paper studies distributed combined authentication and intrusion detection with data fusion in such MANETs. Multimodal biometrics are deployed to work with improved intrusion detection systems (IIDSs) to alleviate the shortcomings of uni-modal 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. The system decides whether user authentication (or IIDS input) is required and which biosensors (or IIDSs) should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IIDS. Simulation results are presented to show the effectiveness of the proposed scheme.

Index Terms—Authentication, biometrics, intrusion detection, mobile ad hoc networks (MANETs), security.

I.INTRODUCTION

With recent advances in mobile computing and wireless communications, mobile ad hoc networks (MANETs) are becoming more attractive for use in military applications. Supporting security-sensitive applications in hostile environments has become an important research area for MANETs since MANETs introduce various security risks due to their open communication medium, node mobility, lack of centralized security services, and lack of prior security association. In high-security MANETs, user authentication is critical in preventing unauthorized users from accessing or modifying network resources. Because the chance of a device in a hostile environment being captured is extremely high, authentication. In high-security MANETs, user authentication is critical in preventing unauthorized users from accessing or modifying network resources. Because the chance of a device in a hostile environment being captured is extremely high, authentication needs to be performed continuously and frequently. The Frequency depends on the situation severity and the resource constraints of the network. User authentication can be performed by using one or more types of validation factors: knowledge factors, possession factors, and biometric factors.

In order to make with users knowledge factors (such as passwords) and possession factors (such as tokens) are very easy to implement but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. Biometrics technology, such as the recognition of finger prints, irises, faces, retinas, etc., provides possible solutions to the authentication problem. Using this technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption.

Due to security inconsistence we using a new technique improved intrusion detection systems s (IIDSs) are important in MANETs to effectively identify malicious activities and so that the MANET may appropriately respond. IIDSs can be categorized as follows. First network-based intrusion detection, which runs at the gateway of a network and examines all incoming packets; Second router-based intrusion detection, which is installed on the routers to prevent intruders from entering the network; and last one host-based intrusion detection, which receives the necessary audit data from the host's operating system and analyzes the generated events to keep the local node secure. For MANETs, host-based IIDSs are suitable since no centralized gateway or router exists in the network. Some research has been done in continuous biometric-based Authentication biometric based continuous authentication is addressed. In dynamic Bayesian networks are used for authentication. Sim et al. Proposed several metrics for multimodal biometrics used for continuous user verification. Some research has been done in combining intrusion detection and continuous authentication in MANETs. In the framework proposed in, multimodal biometrics are used for continuous authentication, and the IIDSs are modeled as sensors to detect the system's security state. The framework is shown to be effective as it combines an important prevention-based security approach and a detection-based approach.

However, the scheme proposed in [9] is a centralized scheme, in which a centralized controller is needed to schedule authentication and intrusion detection, and is more suitable for a single node rather than a network with distributed nodes with random mobility. Since a centralized controller may not be available in MANETs and the centralized scheme can be computationally intractable [10], it is difficult to implement the scheme proposed in [9] for a MANET with distributed nodes.

Second, 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 [11] is used for data fusion.

Third, the system decides whether a user authentication (or IIDS) is required and which biosensors (or IIDS) should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IIDS. Since there is no need for a 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.

And the last 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.

Simulation results are presented to show the effectiveness of the proposed scheme. The main notations used in this paper are summarized in Table I.

The rest of this paper is organized as follows. Section II introduces multimodal biometric-based user authentication and intrusion detection in MANETs. Section III shows how to use Dempster–Shafer theory for the fusion of IIDSs and biometric sensors. The integrated system is formulated in Section IV. Section V shows some simulation results. Finally, we conclude this study with future work in Section VI.

II. RELATED WORKS

This paper studies key management, a fundamental problem in securing mobile ad hoc networks (MANETs). [1] We present IKM, an ID-based key management scheme as a novel combination of ID-based and threshold cryptography. IKM is a certificate less solution in that public keys of mobile nodes are directly derivable from their known IIDS plus some common information. It thus eliminates the need for certificate-based authenticated public-key distribution indispensable in conventional public-key management schemes. IKM features a novel construction method of ID-based public/private keys, which not only ensures high-level tolerance to node compromise, but also enables efficient network-wide key update via a single broadcast message.

When we consider wireless sensor network WSN The energy conservation is the intrinsic issue of the wireless sensor network (WSN). The lack of energy of some necessary sensor nodes will affect the accurate data aggregation as well as the effective lifetime of the network. In this paper,[13] the energy is divided into several energy levels, i.e. different energy ranges of sensor nodes. Since the state of energy level is the random variable with the value of different energy levels at some time the problem of predicting which energy level the WSNs or nodes stay in is addressed. Since the primitive method that exchanges messages through nodes could not directly predict the energy level, the stochastic modeling based on hidden Markov model (HMM) is proposed to solve the problem. which holds the characteristic of the Markov chain, it can be modeled as a left-right HMM. Since the energy level cannot be obtained directly, the energy consumption of sensor nodes at a certain time is used as observation states in HMM

Even though a distributed intrusion-detection system can combine data from multiple nodes to estimate the likelihood of an intrusion, the observing nodes-might not be reliable. [7] The Dempster-Shafer theory of evidence is well suited for this type of problem because it reflects uncertainty. Moreover, Dempster's rule for combination gives a numerical procedure, for fusing together multiple pieces of evidence from unreliable observers. The authors review the Dempster-Shafer theory in the context of distributed intrusion detection and demonstrate the theory's usefulness

In mobile ad hoc networks (MANETs), many applications require group-oriented computing among a large number of nodes in an adversarial environment. To deploy these large-scale cooperative applications, secure multicast service must be provided to efficiently and safely exchange data among nodes. In this paper [2], we propose a pyramidal security model to safeguard the multi security-level information sharing in one cooperation domain. As a prominent feature, a pyramidal security model contains a set of hierarchical security groups and multicast groups. To find an efficient key management solution that covers all the involved multicast groups, we develop the following three schemes for the proposed security model: (1) separated star key graph; (2) separated tree key graph, and (3) integrated tree key graph. Performance comparison demonstrates that the scheme of integrated tree key graph has advantages over its counterparts

To introduce a classification of various mobility models, in addition to proposing the contraction, expansion, and hybrid mobility models. These proposed models[10] cover scenarios in which nodes merge, scatter, or switch to different movement patterns over time. We also investigate a set of mobility metrics to capture characteristics of mobility. We implement our mobility models in the IMPORTANT framework in NS-2. We use our framework to evaluate the performance of ad hoc routing protocols. Our study shows that no one metric is sufficient to capture mobility, but average node degree and link duration are very useful in capturing mobility dynamics. We note a wide spectrum of performance outcomes with mobility. Also, we observe that in some scenarios (involving contraction) performance improves with added velocity.

With the rapid development of wireless technology, various mobile devices have been developed for military and civilian applications. Defense research and development has shown increasing interest in ad-hoc networks because a military has to be mobile. Peer-to-peer is a good architecture for mobile communication in coalition operations. Since there is no need for a dedicated server, users can dynamically route information through the network to anywhere at any time. However, [4] this architecture brings a new challenge in user authentication, which is normally carried out in an authentication server that is absent in ad-hoc networks. In this paper, a biometric authentication model is presented to enhance information security in ad-hoc networks. Using this model, a peer is authenticated with biometrics when joining an existing group even without the presence of an authentication server.

III. PROBLEM AND THE PROBLEM SOLVING APPROACHES

A. EXISTING SYSTEM

When consider a MANETs, environment the security purpose is highly insufficient. Because MANET is a wide area network that any node can enter or leave without any information. Thus user authentication is critical in preventing unauthorized users from accessing or modifying network resources. Because the chance of a device in a hostile environment being captured is extremely high, authentication needs to be performed continuously and frequently. The Frequency depends on the situation severity and the resource constraints of the network. User authentication can be performed by using one or more types of validation factors: knowledge factors, possession factors, and biometric factors.

Knowledge factors (such as passwords) and possession factors (such as tokens) are very easy to implement but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. Biometrics technology, such as the recognition of finger prints, irises, faces, retinas, etc., provides possible solutions to the authentication problem. Using this technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption.

Disadvantages:

i. Misuse detection is the main drawback that it cannot detect new forms of attacks.
ii. Anomaly detection technology is weaker than misuse detection
iii. By analyzing past we found that the system computational complexity is so high.
iv. Thus IIDSs two kinds of errors false positive (FP) and false negative (FN) is one of the important problem that FNs result in security breaches since intrusions are not detected, and therefore, no alert is raised.
v. The false negative rate (FNR) can be used to measure the secure characteristics of the IIDSs since a low FNR implies a low possibility that intrusion occurs without detection.

B. PROPOSED SYSTEM

In this paper, we have presented a distributed scheme combining authentication and intrusion detection. In the proposed scheme, the most suitable biosensors for authentication or IIDSs are dynamically selected based on the current security posture and energy states. The biometric systems operate in authentication mode (one-to-one match process) to address a common security concern: positive verification (the user is whoever the user claims to be). Each biometric system outputs a binary decision: accept or reject.

To improve upon this concept, Dempster–Shafer theory has been used for IIDS and sensor fusion since more than one device is used at each time slot.

Fusion methods include Bayesian fusion methods, fuzzy integrals, Dempster–Shafer combination, fuzzy templates, product of experts, and ANNs. The motivation for selecting Dempster–Shafer theory to solve the fusion problem in our proposed scheme is given as follows [11].

1) It has a relatively high degree of theoretical development for handling uncertainty or ignorance.
2) It provides a convenient numerical procedure for combining disparate data obtained from multiple sources.
3) It is widely used in various applications

Advantages:

1. ANN is a pattern recognition technique with the capacity to adaptively model user or system behavior.
2. DT, which is a useful machine learning technique, is used to organize the attack signatures into a tree structure.
3. By dividing distributed multimodal biometrics authentication and intrusion detection scheduling process into offline and online parts computational complexity can be reduced.
4. With the use of two states: secure state and compromised state a node can be performed well from un-security.

IV. MODULES

1. Biometric-Based User Authentication
2. Improved intrusion detection systems
3. Data fusion of biometric sensors
4. Dempster–Shafer theory
5. Performance analysis

Biometric-Based User Authentication:

Biometric technology can be used to automatically and continuously identify include two kinds of operation models: 1) identification and 2) authentication. In the proposed system, the biometric systems operate in authentication mode (one-to-one match process) to address a common security concern: positive verification (the user is whoever the user claims to be). Based on a comparison of the matching score between the input sample and the enrolled template with a decision threshold

Improved intrusion detection systems :

Intrusion detection is a process of monitoring computer networks and systems for violations of security. Two main technologies of identifying intrusion detection in IIDSs are given as follows: misuse detection and anomaly detection

Data fusion of biometric sensors:

In the proposed scheme, sensors are chosen for authentication and intrusion detection at each time slot to observe the security state of the network. Two

Major fusion based are used, such as class set reduction (CSR) or a class set reordering (CSRR). CSR methods try to find the minimal reduced class set, in which the true class is still represented. CSRR methods try to increase the true class ranking as high as possible. It produce soft outputs, which are the real values in the range [0, 1].

Dempster–Shafer theory:

In a Dempster–Shafer reasoning system, a set of mutually exclusive and exhaustive possibilities is enumerated in the frame of discernment. In this two security states for each node, secure and compromised are used to demonstrate how to use Dempster–Shafer theory in the fusion of biometric sensors and IIDSs.

V. PERFORMANCE ANALYSIS

In this section, we use computer simulations to evaluate the performance of the proposed scheme with and without using data fusion. We consider the following simulation scenario:

A MANET is equipped with two biosensors for continuous authentication, iris sensor, and fingerprint sensor. Each sensor includes two security states, i.e., safe and compromised, and two energy states, i.e., high and low, which means that there are four states for each sensor. The iris sensor is more expensive and also provides more accurate authentication. The fingerprint sensor provides intermediate security authentication and has intermediate energy cost. There is an IIDS in the MANET, which uses the least energy and has the least accuracy in detecting the security state. The following defined matrices are based on the preceding assumptions:

Matrices:

A. Performance Improvement.
B. Network Compromise Probability Improvement.
C. Network Lifetime Improvement and the Optimal Policy.

Performance Improvement:

We run simulations to compare the cost of three approaches: 1) the proposed scheme with data fusion; 2) the proposed scheme without data fusion; and 3) a scheme that does not consider optimal scheduling (that is, a scheme that randomly makes selections). Each cost value is the averaged result of 10 000 simulations. Fig. 3 shows the average cost for the first 100 steps of the simulation. Fig. 4 shows the relative information leakage, which is defined as the information leakage of the selected nodes divided by the information leakage when the nodes are in the worst state.

Network Compromise Probability Improvement:

In these simulations, we investigate the network compromise probability of the proposed scheme. In our simulations, the network is compromised when all of the chosen nodes are in the compromised states. For easy comparison of the network compromise probability in these three schemes, the energy transition probability of each node is set to 1 so that the network dies from being compromised rather than energy exhaustion.

Network Lifetime Improvement and the Optimal Policy

Network lifetime performance has been evaluated for the proposed scheme, which is shown in Fig. 9. To simplify our scheme, data fusion is not applied to the energy state of the nodes. For easy comparison of the network lifetime in different schemes, each node's security transition probability is set to 1 so that the network dies from energy exhaustion in all cases rather than becoming compromised. In these simulations, the network lifetime is defined as the time until all of the chosen nodes are in the low-energy state.

VI. SYSTEM DESIGN

A. System Model

Assume that a MANET has a continuous biometric based authentication system with N − W biosensors and W IIDSs, which have the ability to detect intrusions. The IIDSs are also modeled as sensors, bringing the total number of sensors to N . Without loss of generality, we assume that some nodes have one or more biosensors, and some have no biosensor due to the heterogeneity of network nodes in the MANET. Similarly, some nodes are equipped with the IIDS, and some are not equipped with the IIDS. The total number of network nodes in the MANET is not directly related to the number of sensors. An example framework for the MANET with biosensors and IIDSs is shown in Fig. 1. The system can perform two kinds of operations:

1) Intrusion detection and
2) User authentication.

The IIDSs can operate at all time instants to monitor the system. Authentication may be executed at every time instant as well. However, intrusion detection and authentication may consume a large amount of energy, which is a concern for energy-constrained devices in MANETs. Moreover, performing authentication and intrusion detection may lead to security information leakage to an adversary monitoring communications and network behavior. Therefore, it is critical for the system to optimally schedule the Markov chain for a single node's state transition For example, if there are two security states and two energy states, the state transition probability matrix of each sensor is a 4 * 4 matrix, whose Markov chain.

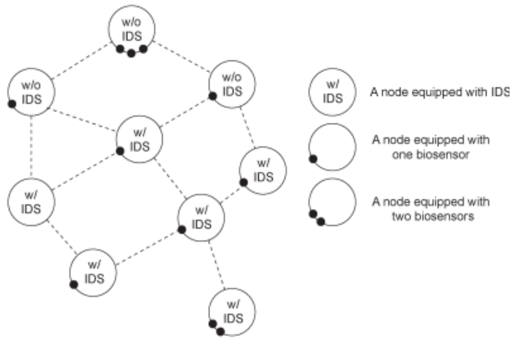

Fig.1. Example framework for a MANET with biosensors and IDSs.

Security- and energy-related costs are considered in our scheme since transmitted biometric information may be detected by adversaries, 1 and energy is certainly consumed when a sensor is used. For example, when cryptographically encoded data (i.e., using public key infrastructure) are sent from biometric sensors to other parts of the biometric systems, an adversary can perform a replay attack: The adversary intercepts the transmitted encrypted data when a genuine user is interacting with the system. The adversary then sends the captured data to the desired biometric parts whenever he wants to break into the system [16].

The simulation result shows the NAM output for the improved intrusion detection systems.

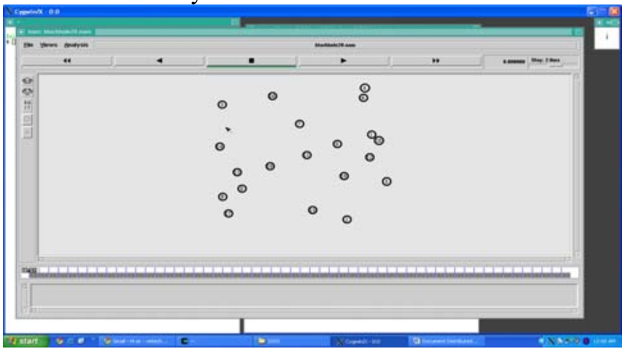

Fig.2. The graphical representation the value of the Quality of Service parameters in the time scale analysis

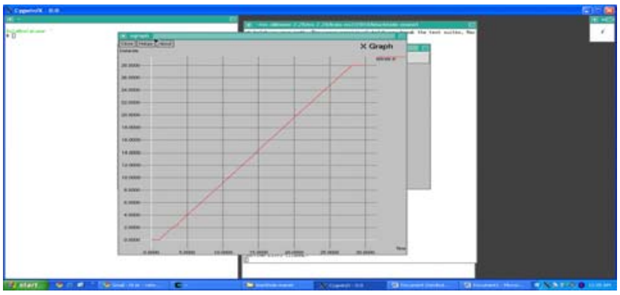

Fig.3. The time based analysis of data rate for the system with improved intrusion detection systems

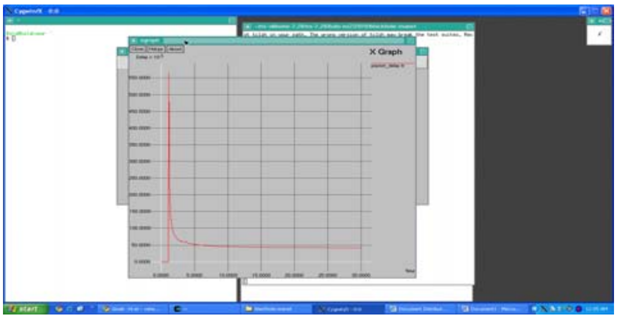

Fig. 4. The delay established in the simulation analysis. The sudden dip in the graph shows the stated going towards the authentication based improved intrusion detection systems

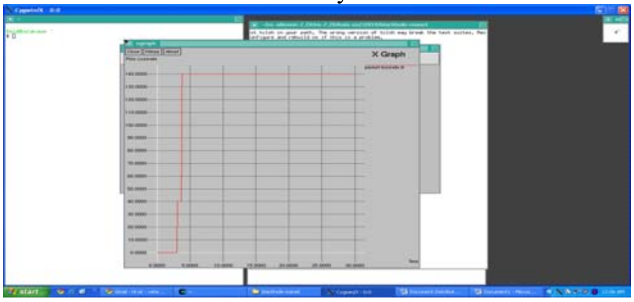

Fig.5. The packet loss rate graph the initial high loss before going for the detection of the intrusion in the system.

VII. CONCLUSION

Combining continuous authentication and intrusion detection can be an effective approach to improve the security performance in high-security MANETs. In this paper, we have presented a distributed scheme combining authentication and intrusion detection. In the proposed scheme, the most suitable biosensors for authentication or IIDSs are dynamically selected based on the current security posture and energy states. To improve upon this concept, Dempster–Shafer theory has been used for IIDS and sensor fusion since more than one device is used at each time slot. The problem has been formulated as a POMDP multi armed bandit problem, and its optimal policy can be chosen using Gittins indexes. The distributed multimodal biometrics and IIDS scheduling process can be divided into offline and online parts to mitigate the computational complex-ity. Simulation results have been presented to show that the proposed scheme can improve network security. Such methods of combining multiple sensor information in a distributed fashion lend themselves well to the concept of cross-layer security, which is a topic that is gaining interest in MANET security.

Future research directions*:*

Further work is in progress to reduce the computation complexity of the proposed scheme by searching for some structured solutions to the distributed scheduling problem.

In addition, we plan to consider more nodes' states, such as mobility and wireless channels, in making the scheduling decisions in MANETs.

Reference:

[1] Y. Zhao, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys,"IEEE Trans. Dependable Secure Com-put. , vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.

[2] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study,"IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398–408, Jan. 2009.

[3] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," IEEE Trans. Pattern Anal. Mach. Intell. vol. 29, no. 4, pp. 687–700, Apr. 2007.

[4] Q. Xiao, "A biometric authentication approach for high security ad-hoc networks," in Proc. IEEE Inf. Assur. Workshop , West Point, NY, Jun. 2004, pp. 250–256.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10]Y. Lu, H. Lin, Y. Gu, and A. Helmy, “Towards mobility rich analysis in ad hoc networks: Using contraction, expansion and hybrid models,” in Proc. IEEE ICC, Paris, France, 2004, pp. 4346–4351.

[11] H. Wu, “Sensor fusion for context-aware computing using Dempster-Shafer theory,” Ph.D. dissertation, Carnegie Mellon Univ., Pittsburgh, PA, 2003.

[12] A. Papanikolaou, C. Ilioudis, C. Georgiadis, and E. Pimenidis, “The importance of biometric sensor continuous secure monitoring,” in Proc. 3rd Int. Conf. Digital Inf. Manage., London, U.K., Nov. 2008.

[13] P. Hu, Z. Zhou, Q. Liu, and F. Li, “The HMM-based modeling for the energy level prediction in wireless sensor networks,” inProc. IEEE Conf. Ind. Electron. Appl. , Harbin, China, May 2007, pp. 2253–2258.