High Security for Manet Using Authentication and Intrusion Detection with Data Fusion

K.K.Lakshmi Narayanan, A.Fidal Castro

***Abstract*—** In Mobile Ad Hoc Network (MANET), Multimodal Biometric technology plays a vital role in giving security between user-to-device authentications. This paper concentrates on the Intrusion Detection and authentication with data fusion in MANET. To overcome the fault in unimodal biometric systems, Multimodal biometrics is set out to work with Intrusion Detection Systems. Each and every device has dimensions and estimation limitations, many devices to be selected and with the help of Dempster-Shafter theory for data fusion observation precision gets increased. Based on the security posture, system concludes which biosensor (IDS) to select and whether user authentication (or IDS input) is essential. By every authentication device and Intrusion Detection System (IDS), the decisions are made in a fully distributed manner. 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

The 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 [3]. 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 [2]. 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 fingerprints, 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. In addition, intrusion detection systems (IDSs) are important in MANETs to effectively identify malicious activities and so that the MANET may appropriately respond. IDSs can be categorized as follows: 1) network-based intrusion detection, which runs at the gateway of a network and examines all incoming packets; 2) router-based intrusion detection, which is installed on the routers to prevent intruders from entering the network; and 3) 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 IDSs are suitable since no centralized gateway or router exists in the network. Some research has been done in continuous biometric-sed authentication. Dynamic Bayesian networks are used for authentication. Proposed [2] several metrics for multimodal biometrics used for continuous user verification. Some research has been done in combining intrusion detection and continuous authentication in MANETs [1]. In the framework proposed in [1], Multimodal biometrics is used for continuous authentication, and the IDSs 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. The Scheme proposed in [1] 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, it is difficult to implement the scheme proposed [1] in for a MANET with distributed nodes. Fully distributed scheme of combining intrusion detection and continuous authentication in MANETs. Several distinct features of the proposed scheme are given here. 1) In the proposed scheme, multimodal biometrics is deployed to alleviate the shortcomings of unimodal biometric systems.

2) 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 [4] is used for data fusion.

3) The system decides whether a user authentication (or IDS) is required and which biosensors should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IDS. 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.

4) 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.

II. AUTHENTICATION AND INTRUSION DETECTION

In this section, biometric-based user authentication and IDSs are used in MANETs. Then the system model is shown.

A. Biometric-Based User Authentication

Biometric technology can be used to automatically and continuously identify or verify individuals by their physiological or behavioral characteristics. Biometric systems 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). In most real-world implementations of biometric systems, biometric templates are stored in a location remote to the biometric sensors. In biometric authentication processes, two kinds of errors can be made: 1) false acceptance (FA) and 2) false rejection (FR). FAs result in security breaches since unauthorized persons are admitted to access the system/network.

FRs result in convenience problems since genuinely enrolled identities are denied access to the system/network, and maybe some further checks need to be done. The frequency of FA errors and of FR errors is called FA rate (FAR) and FR rate (FRR), respectively. The FAR can be used to measure the security characteristics of the biometric systems since a low FAR implies a low possibility that an intruder is allowed to access the system/network. In tactical MANETs, failure in user authentication might result in serious consequences. Hence, more than one biometric sensor is used at each time period in our system to increase the effectiveness of user authentication.

B.IDSs

Intrusion detection is a process of monitoring computer networks and systems for violations of security and can be automatically performed by IDSs [5]. Two main technologies of identifying intrusion detection in IDSs are given as follows: 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 [5]. Multiple algorithms have been applied to model attack signatures or normal behavior patterns of systems. Three common algorithms are naive Bayes, artificial neural network (ANN), and decision tree (DT). A naive Bayes classifier is based on a probabilistic model to assign the most likely class to a given instance. ANN is a pattern recognition technique with the capacity to adaptively model user or system behavior.

DT, which is a useful machine learning technique, is used to organize the attack signatures into a tree structure. Most of the IDSs only use one of the preceding algorithms. IDSs can make two kinds of errors: false positive (FP) and false negative (FN). FNs result in security breaches since intrusions are not detected, and therefore, no alert is raised. The false negative rate (FNR) can be used to measure the secure characteristics of the IDSs since a low FNR implies a low possibility that intrusion occurs without detection.

III. DATA FUSION

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. It can be quite difficult to ascertain which observers are compromised. Therefore, choosing an appropriate fusion method is critical for the proposed scheme. Existing fusion methods can be classified as follows based on the output information level of the base classifiers:

Type-I

Classifiers output single-class labels (SCLs). Majority voting and behavior-knowledge space are two most representative methods for fusing SCL classifiers. Majority voting can operate under the assumption that most of the observing nodes are trustworthy.

Type-II

Classifiers output class rankings. Two major fusion methods of type-II classifiers' outputs are based on either a 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.

Type-III

Classifiers produce so-called soft outputs, which are the real values in the range [0, 1]. Fusion methods for type-III classifiers try to reduce the uncertain level and maximize suitable measurements of evidence. Fusion methods include Bayesian fusion methods, fuzzy integrals, Dempster–Shafer combination, fuzzy templates, product of experts, and ANNs. The Dempster–Shafer evidence theory was originated by Dempster and later revised by Shafer. Its essential idea is that an observer can obtain degrees of belief about a proposition from a related proposition's subjective

probabilities. The motivation for selecting Dempster–Shafer theory [4] to solve the fusion problem in our proposed scheme is given as follows.

1) It has a relatively high degree of theoretical development for handling uncertainty or ignorance.

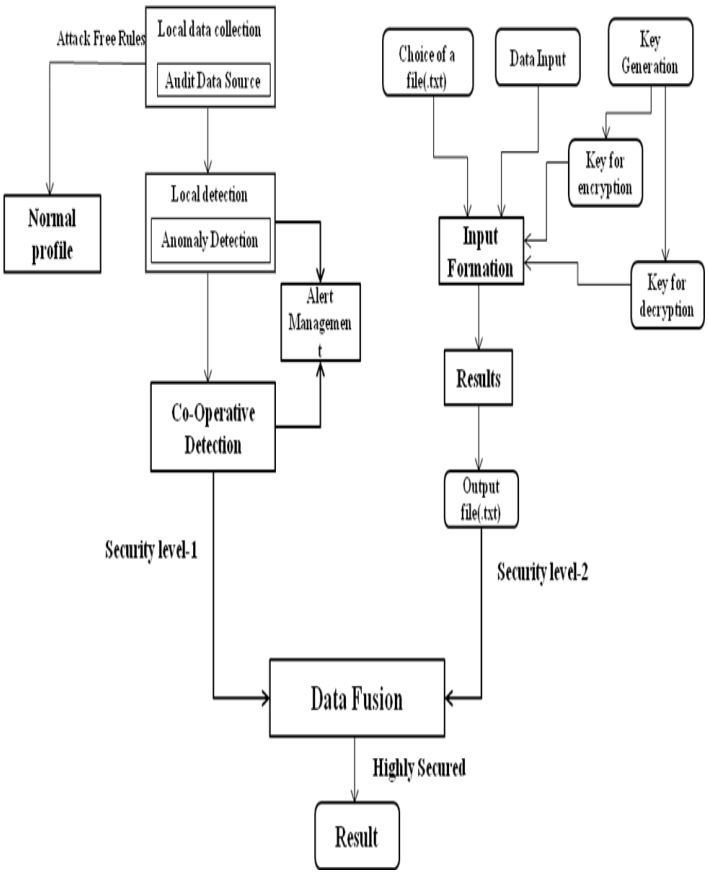
2) It provides a convenient numerical procedure for combining disparate data obtained from multiple sources.

3) It is widely used in various applications. In a Dempster–Shafer reasoning system, a set of mutually exclusive and exhaustive possibilities is enumerated in the frame of discernment, which is denoted by Ω [4]. In this section, two security states for each node, i.e., {secure, compromised}, are used to demonstrate how to use Dempster–Shafer theory in the fusion of biometric sensors and IDSs. Note that the theory can be applied for nodes with more than two security states. In the proposed scheme, the frame of discernment consists of two possibilities concerning the security state of an arbitrary node *a*. That is, Ω={secure, compromised}, which presents that node *a* has two security states: 1) Secure state & 2) Compromised state.

If these biometric sensors observe with different accuracies, the weighted Dempster-Shafer evidence combining rule is used in Dempster–Shafer evidence combination.

Based on the historical performances of the sensors in similar situations, their corresponding correctness rates are used as the references to decide how much the sensors' current estimations should be trusted from their current observation. Let *wb* and *wc* be the corresponding estimation correctness rates in history for *b* and *c*, respectively. Then, the combined belief of biometric sensors *b* and *c* can be calculated. If more than two sensors are chosen at each time slot, the evidence can be computed by combining any pair of arguments and then combining the results with the remaining arguments. Since inaccurate detection is the main characteristic of untrustworthy sensors, only detection errors are considered in the proposed scheme.

IV. ARCHITECTURE



Architecture Diagram

V. FORMULATION

It is critical for the system to optimally schedule the intrusion detection and authentication activities for each time slot in a distributed manner, taking system security and energy into account. The distributed authentication and intrusion detection scheduling problem as a partially observable Markov decision process (POMDP) multiarmed bandit problem.

A. Information State Formulation

The decision about which sensors are chosen should not totally depend on the current observation values since the sensors' states are only partially observable. Therefore, all the actions and observations in the history should be counted as a basis for decision making under environmental uncertainties. The information state of a sensor refers to a probability distribution over the sensor's states. The entire probability space (the set of all possible probability distributions) is referred to as the information space. For an arbitrary sensor n, the information state at time k is denoted as $\pi(n)$.

B. Distributed Scheduling Process

To reduce the computational complexity of the proposed scheme, the distributed multimodal biometrics authentication and intrusion detection scheduling process can be divided into offline and online parts.

1) Offline computation of Gittins index. As with any dynamic programming formulation, the computation of the Gittins index for each sensor can be done offline. For an arbitrary sensor n, a set of vectors Λ(n) k at each iteration k is computed in advance based on the following parameters: state transition probability matrix $T(n)$, observation probability matrix $B(n)$, reward vector $R(n)$, initial information state $\pi(n)$ 0 , horizon length H, and discount factor β.

2) Real-time sensor selection over horizon H. At time k, each sensor stores the sensors' current Gittins indexes into an N-dimensional vector. The real-time sensor selection includes the following steps.

a) Select L sensors with the highest Gittins indexes at time k. For these L sensors, perform steps a to e.

b) Get new sensor observations $y(n)$ k+1 at time k + 1.

c) Update the information states of the L chosen sensors using the corresponding HMM filters.

d) Compute the Gittins index γ (n) H $(\pi$ (n) k+1) for each of these L sensors only.

e) Broadcast the new Gittins indexes to the other sensors.

f) On receiving the messages, all the sensors update their Gittins indexes. Go to step a.

C. Computational Complexity and Communication Overhead

The optimal policy can be found by a Gittins index rule, which means that the scheduling problem only needs to solve the individual POMDPs for each sensor. Therefore, the computational complexity of the proposed scheme is dramatically decreased. A lookup table can be designed with little computational complexity. For example, based on Lovejoy's suboptimal algorithm, the value function can be upper and lower bounded, and efficient suboptimal solutions can be developed. Finally, by imposing structural assumptions on the state transition probabilities, cost vectors, and observation probabilities, some structural policies (e.g., threshold policy) can be derived. In the proposed scheme, communication overhead is mainly due to multicasting the following two types of messages in the real-time scheduling process:

1) INTIAL-SENSOR-INDICES (ISIND), 8 bytes, which is sent at the beginning of the authentication and intrusion detection process, so that each sensor knows the others' Gittins indexes;

2) SENSOR-INDICES (SIND), 8 bytes, which is sent at the beginning of each time slot by the L nodes active in the previous time slot. Any network layer multicast algorithm for ad hoc networks can be used in the scheme. The proposed scheme's total communication overhead is proportional to $8N \times (N - 1)$ bytes plus $8L \times (N - 1)$ bytes per time slot. Overall, the proposed scheme's communication overhead is similar to that of the centralized scheme, as they are both bounded by $O(LN)$.

VI. Conclusion:

Combining continuous authentication and intrusion detection can be an effective approach to improve the security performance in high-security MANETs. In this paper, a distributed scheme combining authentication and intrusion detection. In the proposed scheme, the most suitable biosensors for authentication or IDSs are dynamically selected based on the current security posture and energy states. To improve upon this concept, Dempster–Shafer theory has been used for IDS and sensor fusion since more than one device is used at each time slot. The problem has been formulated as a POMDP multiarmed bandit problem, and its optimal policy can be chosen using Gittins indexes. The distributed multimodal biometrics and IDS scheduling process can be divided into offline and online parts to mitigate the computational complexity. 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.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

[5] A. Mishra, K. Nadkarni, and V. T. A. Patcha, "Intrusion detection in wireless ad-hoc networks," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 48–60, Feb. 2004.