Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks

Shengrong Bu, *Student Member, IEEE*, F. Richard Yu, *Senior Member, IEEE*, Xiaoping P. Liu, *Senior Member, IEEE*, Peter Mason, and Helen Tang, *Member, IEEE*

***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 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. The system decides whether user authentication (or IDS input) is required and which biosensors (or IDSs) should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IDS. 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 [1], [2].

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 [3]. The frequency depends on the situation severity and the resource constraints of the network [3]. 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 [4]. Using this technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption [4], [5].

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 [6]: 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-based authentication. In [3], [5], [7], and [8], biometric-based continuous authentication is addressed. In [8], dynamic Bayesian networks are used for authentication. Sim *et al.* [3] 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 [9]. In the framework proposed in [9], multimodal biometrics are 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. 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

Manuscript received June 15, 2010; revised October 24, 2010; accepted December 1, 2010. Date of publication December 30, 2010; date of current version March 21, 2011. This work was supported by the Natural Sciences and Engineering Research Council of Canada, Defence R&D Canada, and industrial and government partners through the Healthcare Support through the Information Technology Enhancements Strategic Research Network. The review of this paper was coordinated by Dr. L. Chen.

S. Bu, F. R. Yu, and X. P. Liu are with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: shengrbu@sce.carleton.ca; pliu@sce.carleton.ca; richard_yu@carleton.ca).

P. Mason and H. Tang are with Defence Research and Development Canada, Ottawa, ON K1A 0Z4, Canada (e-mail: peter.mason@drdc-rddc.gc.ca; helen.tang@drdc-rddc.gc.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2010.2103098

TABLE I
MAIN NOTATIONS

Symbol	Meaning
$x_k^{(n)} = \left[s_k^{(n)}, e_k^{(n)}\right]$	The state of sensor n at time slot k
$s_k^{(n)}$	The security state of sensor n at time slot k
$e_k^{(n)}$	The residual energy state of sensor n at time slot k
$T^{(n)} = U^{(n)} \otimes V^{(n)}$	The state transition probability matrix of the state of sensor n
$U^{(n)}$	The state transition probility matrix of the security state of sensor n
$V^{(n)}$	The state transition probability matrix of the residual energy state of sensor n
C_k	The total instantaneous cost at time k
$y_{k+1}^{(n)}$	Observation obtained from node n at time $k+1$
$\pi_k^{(n)}$	The information state of sensor n at time k
$B^{(n)}$	The observation probability matrix of node n
Y_k	The observation history at time k
A_{k-1}	The action history at time k

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.

In this paper, we propose a 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 are 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 [11] is used for data fusion.
3) The system decides whether a user authentication (or IDS) is required and which biosensors (or IDS) 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. 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 IDSs 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. MULTIMODEL BIOMETRIC-BASED USER AUTHENTICATION AND INTRUSION DETECTION

In this section, we introduce biometric-based user authentication and IDSs used in MANETs. Then, we present the system model in this paper.

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). 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. In most real-world implementations of biometric systems, biometric templates are stored in a location remote to the biometric sensors [12].

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 are 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. Two main technologies of identifying intrusion detection in IDSs are given as follows: misuse detection and anomaly detection [13]. 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 [13].

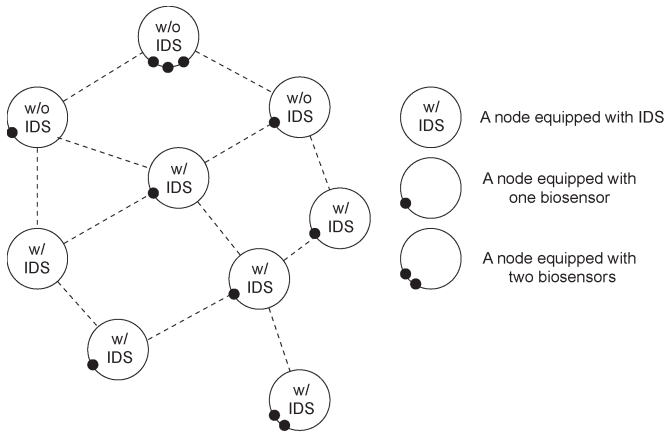

Fig. 1. Example framework for a MANET with biosensors and IDSs.

Multiple algorithms have been applied to model attack signatures or normal behavior patterns of systems. Three common algorithms are [14] 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.

C. System Model

Assume that a MANET has a continuous biometric-based authentication system with $N-W$ biosensors and W IDSs, which have the ability to detect intrusions. The IDSs 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 IDS, and some are not equipped with the IDS. 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 IDSs is shown in Fig. 1.

The system can perform two kinds of operations: 1) intrusion detection and 2) user authentication. The IDSs 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 intrusion detection and authentication activities for each time slot, taking system security and energy into account.

In the proposed scheme, since each sensor (biosensor or IDS) has measurement and estimation limitation, more than one biosensor and IDS (assume L devices) is chosen to detect the security states of the system. Each sensor monitors its local environment and not other sensors'. Then, their observations can be fused to increase observation accuracy using Dempster–Shafer theory. The number of sensors chosen is determined by the required level of network performance.

In the proposed scheme, a Markov model is used. Let the state of an arbitrary sensor n, $n \in \{1, 2, \ldots, N\}$ be $x^{(n)}(t)$ at time t, which includes the sensor security and energy states $[s^{(n)}(t), e^{(n)}(t)]$. Each state represents the security condition and the residual battery energy level of sensor n at time t. For example, security state space I can include two security levels: $\{safe, compromised\}$. The residual battery energy of each sensor can be divided into h discrete levels. Therefore, the residual energy state space $\mathcal{E}$ includes energy states $\{e_1, \ldots, e_h\}$ [15]. For example, the residual energy state space $\mathcal{E}$ can include two energy levels: $\{High, Low\}$.

We consider that the time axis is divided into equal time slots, which correspond to the time intervals between two continuous user authentications. Let $x_k^{(n)}$, $s_k^{(n)}$, and $e_k^{(n)}$ denote the state of sensor n, its security state, and its residual energy state, respectively, at discrete time $k = 0, 1, \ldots$. States $s_k^{(n)}$ and $e_k^{(n)}$ evolve based on I-state and $\mathcal{E}$-state Markov chains with transition probability matrices $U^{(n)}$ and $V^{(n)}$, respectively, if sensor n is used at time k, which are described as follows:

$$U^{(n)} = \left(\phi_{ij}^{(n)}\right)_{i,j\in I} \tag{1}$$

$$V^{(n)} = \left(\psi_{ij}^{(n)}\right)_{i,j\in \mathcal{E}} \tag{2}$$

where

$$\phi_{ij}^{(n)} = P\left(s_{k+1}^{(n)} = j | s_k^{(n)} = i\right)$$

and

$$\psi_{ij}^{(n)} = P\left(e_{k+1}^{(n)} = j | e_k^{(n)} = i\right)$$

respectively.

The states of other idle sensors are unchanged, i.e., $s_{k+1}^{(n)} = s_k^{(n)}$ and $e_{k+1}^{(n)} = e_k^{(n)}$, if sensor n is idle at time k. Hence, the state of sensor n transitions with probability matrix $T^{(n)} = [U^{(n)} \otimes V^{(n)}]$, where $\otimes$ denotes the Kronecker product. 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 is shown in Fig. 2.

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

[1]Even if this information is encrypted, the fact that it is being transmitted conveys information to an adversary.

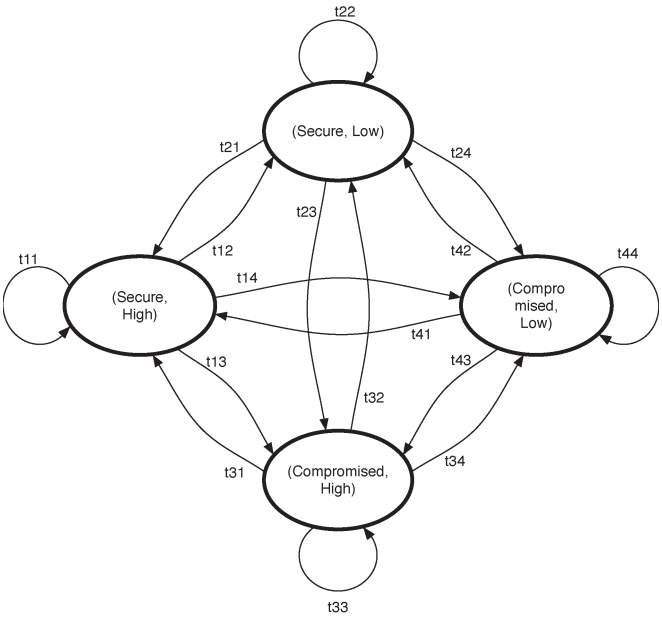

Fig. 2. Example of Markov chain for a single node's state transition.

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].

Let $a_k \in \{1, \ldots, N\}$ denote one chosen sensor at time k. Its corresponding information leakage cost at time k is defined as $c_s(s_k^{(a_k)}, a_k)$, which is a function of the security state of the chosen sensor and action at that time. The corresponding energy cost at time k is defined as $c_e(e_k^{(a_k)}, a_k)$, which is a function of the energy state of the chosen sensor and action at that time. If sensor n is used at time k, an instantaneous cost $\beta^k c(x_k^{(n)}, n)$ is accrued, where $c(x_k^{(n)}, n) = (1 - \lambda)c_s(s_k^{(n)}, n) + \lambda c_e(e_k^{(n)}, n)$, with $\lambda \in (0, 1)$ being the weight factor for these two kinds of costs. β $(0 \leq \beta < 1)$ denotes the discount factor, which is needed to make the infinite sum mathematically converge in (4) [17], [18]. The discount factor can model the fact that future cost is worth less than immediate cost, because the future is less certain. In the proposed scheme, the total instantaneous cost C_k at time k is determined as follows: Define a set $SL \subseteq \{1, \ldots, N\}$, $|SL| = L$, i.e.,

$$C_k = \beta^k \times \sum_{n=1}^{L} c\left(x_k^{(n)}, n\right), n \in SL. \tag{3}$$

The total expected discounted cost over an infinite-time horizon is given by

$$J_\mu = E\left[\sum_{k=0}^{\infty} C_k\right]. \tag{4}$$

The optimization objective is to find the optimal stationary policy $\mu^* = \arg\min_{\mu \in \eta} J_\mu$ to minimize the cost in (4).

III. Data Fusion of Biometric Sensors and Intrusion Detection Systems

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. (How to optimally schedule the L sensors is presented in Section IV.) 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.

Existing fusion methods can be classified as follows based on the output information level of the base classifiers [19]: 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 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.

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 [20]. 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, $\Omega = \{secure, compromised\}$, which presents that node a has two security states: 1) secure state and 2) compromised state. Any hypothesis H refers to a subset of Ω for which the neighboring biometric sensors and IDSs can present evidence. The set of all possible subsets of Ω,

including itself and the null set, is called a power set and is designated as 2^{Ω} [20]. For Ω in the proposed scheme, the power set has three focal elements: 1) hypothesis $H = \{secure\}$; 2) hypothesis $\bar{H} = \{compromised\}$; and 3) hypothesis $U = \Omega$, which means that the observed sensor a is either in the secure state or the compromised state. Each biometric sensor and IDS contributes its observation by assigning its beliefs over Ω.

In this paper, if a sensor is *trustworthy*, then the sensor always provides 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 $P(s_{k+1}^{(n)} = secure) \times P(y_{k+1}^{(n)} = s_{k+1}^{(a)})$, where $y_{k+1}^{(n)}$ is the observation of a's security state obtained from node n. In our scheme, $P(y_{k+1}^{(n)} = secure | s_{k+1}^{(a)} = secure)$ and $P(y_{k+1}^{(n)} = compromised | s_{k+1}^{(a)} = compromised)$ are equal to $1 - FAR$ and $1 - FRR$, respectively. FAR and FRR are the frequencies of FA errors and FR errors for node n, respectively. Otherwise, node n is not trustworthy with probability $1 - tp_{k+1}^{(n)}$. Suppose that node n states that node a is secure. If node n is trustworthy, then its claim is accurate. If n is not trustworthy, its claim is not necessarily inaccurate.

Basic probability assignment reflects the evidence's strength of support [20]. For example, for node n, the basic probability number $m_n(H)$ is defined as the portion of total belief assigned to hypothesis H [20]. When $n's$ observation data $y_{k+1}^{(n)}$ for the security state of node a at time $k+1$ are equal to $secure$, its basic probability assignment can be calculated as follows [20]:

$$\begin{aligned} m_n(H) &= P\left(s_{k+1}^{(n)} = secure\right) \\ &\quad \times P\left(y_{k+1}^{(n)} = secure | s_{k+1}^{(a)} = secure\right) \\ m_n(\bar{H}) &= P\left(s_{k+1}^{(n)} = secure\right) \\ &\quad \times P\left(y_{k+1}^{(n)} = secure | s_{k+1}^{(a)} = compromised\right) \\ m_n(U) &= P\left(s_{k+1}^{(n)} = compromised\right). \end{aligned} \tag{5}$$

If node n claims that node a is compromised, its basic probability assignment can be calculated as follows [20]:

$$\begin{aligned} m_n(H) &= P\left(s_{k+1}^{(n)} = secure\right) \\ &\quad \times P\left(y_{k+1}^{(n)} = compromised | s_{k+1}^{(a)} = secure\right) \\ m_n(\bar{H}) &= P\left(s_{k+1}^{(n)} = secure\right) \\ &\quad \times P\left(y_{k+1}^{(n)} = compromised | s_{k+1}^{(a)} = compromised\right) \\ m_n(U) &= P\left(s_{k+1}^{(n)} = compromised\right). \end{aligned} \tag{6}$$

In the remainder of this section, two biometric sensors b and c are used to demonstrate how to apply Dempster–Shafer theory in combining the belief m_b of sensor b and the belief m_c of sensor c in the hypotheses. When these two biometric sensors have the same accuracy estimations or they are in situations where their probability assignments over the frame of discernment can quantitatively reflect the ignorance of each other's observations, the *equally trusting approach* is used in Dempster–Shafer evidence combination [20]. The combined belief of sensors b and c can be calculated as follows [20]:

$$\begin{aligned} m_b(H) \oplus m_c(H) &= \frac{1}{K}\left[m_b(H)m_c(H)\right. \\ &\quad \left. + m_b(H)m_c(U) + m_b(U)m_c(H)\right] \\ m_b(\bar{H}) \oplus m_c(\bar{H}) &= \frac{1}{K}\left[m_b(\bar{H})m_c(\bar{H})\right. \\ &\quad \left. + m_b(\bar{H})m_c(U) + m_b(U)m_c(\bar{H})\right] \\ m_b(U) \oplus m_c(U) &= \frac{1}{K} m_b(U)m_c(U) \end{aligned} \tag{7}$$

where

$$\begin{aligned} K = {} & m_b(H)m_c(H) + m_b(H)m_c(U) + m_b(U)m_c(U) \\ & + m_b(U)m_c(H) + m_b(U)m_c(\bar{H}) \\ & + m_b(\bar{H})m_c(\bar{H}) + m_b(\bar{H})m_c(U). \end{aligned} \tag{8}$$

If these biometric sensors observe with different accuracies, the *weighted Dempster-Shafer evidence combining rule* is used in Dempster–Shafer evidence combination [11]. 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 w_b and w_c 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 as follows [11]:

$$\begin{aligned} m_b(H) \oplus m_c(H) &= \frac{1}{K}\left[w_b m_b(H) w_c m_c(H)\right. \\ &\quad + w_b m_b(H) w_c m_c(U) \\ &\quad \left. + w_b m_b(U) w_c m_c(H)\right] \\ m_b(\bar{H}) \oplus m_c(\bar{H}) &= \frac{1}{K}\left[w_b m_b(\bar{H}) w_c m_c(\bar{H})\right. \\ &\quad + w_b m_b(\bar{H}) w_c m_c(U) \\ &\quad \left. + w_b m_b(U) w_c m_c(\bar{H})\right] \\ m_b(U) \oplus m_c(U) &= \frac{1}{K} w_b m_b(U) w_c m_c(U) \end{aligned} \tag{9}$$

where

$$K = 1 - w_a w_b \left[m_a(H)m_b(\bar{H}) + m_a(\bar{H})m_b(H)\right]. \tag{10}$$

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. Formulation of the Distributed Authentication and Intrusion Detection Scheduling Problem

As we mentioned in the introduction, 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. In this section, we formulate the distributed authentication and intrusion detection scheduling problem as a partially observable Markov decision process (POMDP) multiarmed bandit problem [17], [21].

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. To this end, *information state* is developed to derive sufficient statistical information for the past history, including all the actions and observations. 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 $\pi_k^{(n)}$, i.e.,

$$\pi_k^{(n)} = \left(\pi_k^{(n)}(i)\right), \qquad i = 1, \ldots, \zeta_n \tag{11}$$

where

$$\pi_k^{(n)}(i) = P\left(x_k^{(n)} = i | Y_k, A_{k-1}\right)$$

and

$$1'_{\zeta_n} \pi^{(n)} = 1.$$

In the preceding equation, $Y_k = (y_1^{(a_0)}, \ldots, y_k^{(a_{k-1})})$ and $A_{k-1} = (a_0, \ldots, a_{k-1})$ denote the observation and action (sensor selection) history, respectively, at time k. 1_{ζ_n} is an ζ_n-dimensional column vector of ones.

If sensor n is chosen at time k, a new observation $y_{k+1}^{(n)}$ is obtained at time $k+1$. Furthermore, an essential part of information state is that it can be updated after each corresponding action to incorporate one additional step of information into the history. Specifically, the information state at that time $\pi_{k+1}^{(n)}$ can be recursively updated by the hidden Markov model (HMM) state filter known as the *forward algorithm* with the new observation, i.e., [21]

$$\pi_{k+1}^{(n)} = \frac{B^{(n)}\left(y_{k+1}^{(n)}\right) T^{(n)\prime} \pi_k^{(n)}}{1'_{\zeta_n} B^{(n)}\left(y_{k+1}^{(n)}\right) T^{(n)\prime} \pi_k^{(n)}} \tag{12}$$

where $B^{(n)}$ denotes the observation probability matrix of node n, which denotes the probabilities of the observation $y_{k+1}^{(n)}$ acquired when sensor n is picked at time $k+1$, given each state of the Markov chain. When L nodes are used, the observation probability matrix is obtained by using the preceding Dempster–Shafer evidence combining rules. Since the other $N-L$ sensors are not used at time k, their information states remain unchanged at time $k+1$.

The preceding POMDP multiarmed bandit problem can be re-expressed as a fully observable multiarmed bandit problem in terms of the information state, which means optimal sensors can be chosen based on the information state [18]. This is because, although the state of each sensor is not totally observable, its information state space is totally observable. Generally, we need to solve N-POMDP with large computational complexity. However, it is proven that an *indexable* property exists that can dramatically simplify the computation and implementation of the optimal policy, meaning that the optimal policy can be found according to the Gittins indexes [18] of the sensors. Sensors' Gittins indexes $\gamma^{(n)}(\pi_k^{(n)})(n = 1, \ldots, N)$ are used to choose the appropriate sensors at time k [18]. Therefore, the optimal policy at time k is that the L sensors with the largest Gittins indexes at that time should be selected. The aforementioned problem can be transformed to compute the Gittins index of each sensor. A finite-dimensional value iteration algorithm proposed in [21] is used to compute the Gittins index for each sensor.

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 $\Lambda_k^{(n)}$ 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 $\pi_0^{(n)}$, 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 $y_{k+1}^{(n)}$ at time $k+1$.
   c) Update the information states of the L chosen sensors using the corresponding HMM filters.
   d) Compute the Gittins index $\gamma_H^{(n)}(\pi_{k+1}^{(n)})$ 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. Discussion of Computational Complexity and Communication Overhead

In the proposed scheme, 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. For online real-time scheduling of different sensors, each sensor just looks up the prebuilt index table to find the index value corresponding to the current state. A lookup table can be designed with little computational complexity. In addition, several computationally efficient algorithms can be found in [22] to further reduce the computational complexity of the proposed scheme. For example, based on Lovejoy's suboptimal algorithm, the value function can be upper and lower bounded, and efficient suboptimal solutions can be developed [23]. 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 [24].

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 $O(LN)$.

V. Simulation Results and Discussions

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 IDS 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:

The security state transition matrices of the iris sensor, fingerprint sensor, and IDS, when they are active, are defined as follows:

$$U^{(1)} = \begin{pmatrix} 0.95 & 0.05 \\ 0.30 & 0.70 \end{pmatrix}, \quad U^{(2)} = \begin{pmatrix} 0.80 & 0.20 \\ 0.10 & 0.90 \end{pmatrix}$$

$$U^{(3)} = \begin{pmatrix} 0.98 & 0.02 \\ 0.02 & 0.98 \end{pmatrix}.$$

From these state transition matrices, we can see the probability of changing from one state to another. For example, the iris sensor could be compromised with probability 0.05 and retrieved back to the safe state with probability 0.30. The corresponding energy state transition matrices are defined as

$$V^{(1)} = \begin{pmatrix} 0.96 & 0.04 \\ 0 & 1 \end{pmatrix}, \quad V^{(2)} = \begin{pmatrix} 0.98 & 0.02 \\ 0 & 1 \end{pmatrix}$$

$$V^{(3)} = \begin{pmatrix} 0.99 & 0.01 \\ 0 & 1 \end{pmatrix}$$

which means that, when the battery residual energy is low, it cannot transition back to the high-energy level. The observation matrices for the security state and energy state are defined as

$$B_s^{(1)} = \begin{pmatrix} 0.97 & 0.03 \\ 0.03 & 0.97 \end{pmatrix}, \quad B_s^{(2)} = \begin{pmatrix} 0.90 & 0.10 \\ 0.10 & 0.90 \end{pmatrix}$$

$$B_s^{(3)} = \begin{pmatrix} 0.80 & 0.20 \\ 0.20 & 0.80 \end{pmatrix}, \quad B_e = \begin{pmatrix} 0.90 & 0.10 \\ 0.10 & 0.90 \end{pmatrix}$$

respectively.

The cost matrices are defined as $C(1) = (3, 8, 25, 27)$, $C(2) = (2, 7, 20, 26)$, and $C(3) = (1, 4, 27, 31)$. Since there is more potential for information leakage when a node is in the compromised state than in the safe state, the information leakage cost of selecting a safe node is lower than that of selecting a compromised node.[2] When the network is compromised, an extra cost C_{net} is applied into the total cost. In our simulation, C_{net} is set to 30 based on the nodes' cost matrices, although different values could be chosen without affecting the results of our comparisons.

It is a nontrivial task to set up transition matrices and cost matrices for the proposed scheme. We assume that most nodes' properties can be made known when constructing these matrices, which should be realistic particularly for tactical MANETs where initial device management and planning is an *a priori* requirement. By "node properties," we mean the information and states that are used as inputs to the transition and cost matrices. However, in a dynamic environment, where heterogeneous nodes may join the network, it may not be realistic to assume knowledge of all nodes' properties. In these circumstances, we should be able to predict and learn the nodes' properties from the history of observations and actions.

We used "pomdp-solve," which is a program in C++ from [25], to compute the set of vectors $\wedge_H$ required for the algorithm in [21]. In pomdp-solve, we chose the *incremental pruning algorithm* developed in the artificial intelligence community by Cassandra *et al.* [22] since it is one of the fastest algorithms

[2]For example, a compromised node could intentionally introduce collisions in a cryptographic protocol.

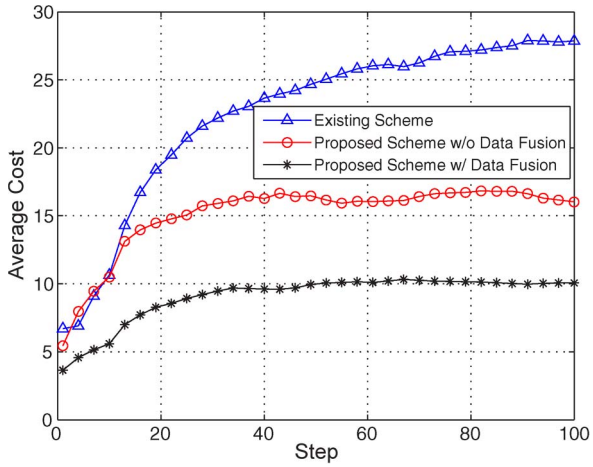

Fig. 3. Cost comparison among the proposed scheme with data fusion, the proposed scheme without data fusion, and the existing scheme.

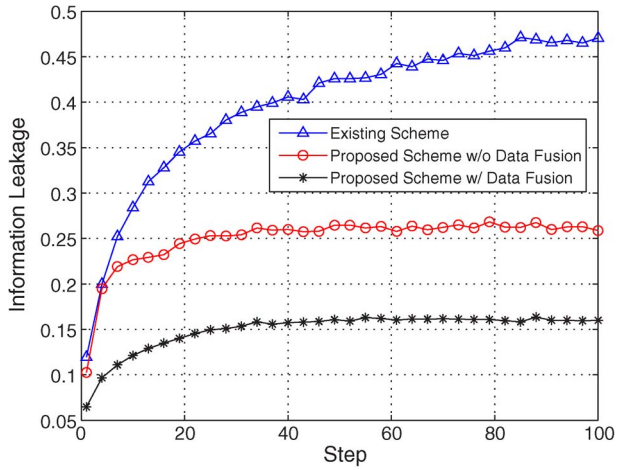

Fig. 4. Information leakage comparison among three schemes.

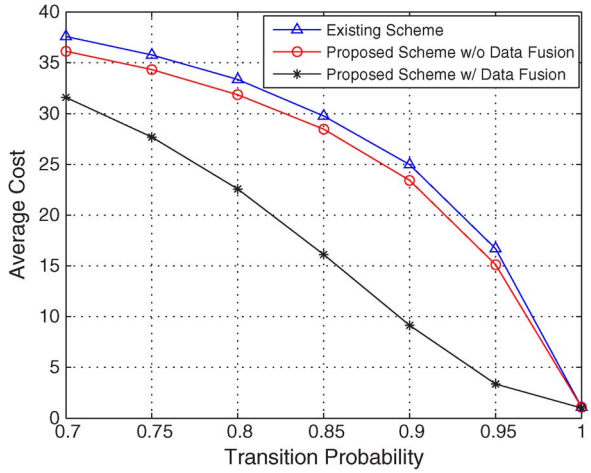

Fig. 5. Cost comparison among three schemes under different transition probabilities.

for solving POMDPs [10]. We implemented the computation of the Gittins indexes in Matlab. All simulations are run, and policy vectors are computed on a computer equipped with Window 7, Intel Core 2 Duo P8400 CPU (2.26GHz), and 4-GB memory. In the simulations, the initial state for each node is of high energy and secure. We adopt the hybrid Manhattan and RWP mobility model [26] to simulate the nodes moving. Block Rayleigh flat-fading wireless channel model [27] is used in this paper.

A. *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. The results show that the proposed scheme with data fusion and the proposed scheme without data fusion have lower cost and less information leakage than the existing scheme. Thus, through optimal node selection, the system can be more secure and energy efficient. From these figures, we can observe that data fusion can improve performance. The reason the fusion scheme has better performance is that data fusion using Dempster–Shafer theory increases the observation accuracy by combining the observations from multiple sensors.

Various transition probabilities are also used in the simulations to evaluate the dynamic stability of the proposed scheme. Fig. 5 shows the average cost of these three schemes when the first component in the security transition probability matrix varies from 0.7 to 1.0, where high transition probability means that the system is more secure. The results still show that the proposed scheme with data fusion has the lowest cost among these three schemes. From Fig. 5, we can also see that the cost decreases when the system becomes more secure. This is because the information leakage is smaller when the system becomes more secure; therefore, the cost is smaller. When the security transition probability reaches 1, the proposed schemes lose their advantages since all of the nodes always stay in the secure states, that is, there is no added value in trying to optimize security in an infallible network. Fig. 6 shows the average information leakage within the first 40 steps when the first component in the security transition probability matrix of the IDS varies from 0.65 to 0.95 and all other probability values remain constant. Results show that the information leakage of the proposed schemes remains low and stable. The reason for this is that the proposed schemes avoid choosing the compromised nodes and therefore decrease information leakage and network compromise probability.

Different numbers of nodes are also used in the simulations to verify the scalability of the proposed scheme. Fig. 7 shows the average cost within the first 100 steps of the simulations of networks of different sizes. In these simulations, we use the same three kinds of nodes mentioned earlier. Results show that the proposed scheme with data fusion has the lowest cost compared with the existing scheme and the proposed scheme without data fusion. The results also show that the cost of the proposed schemes and existing scheme decreases when the

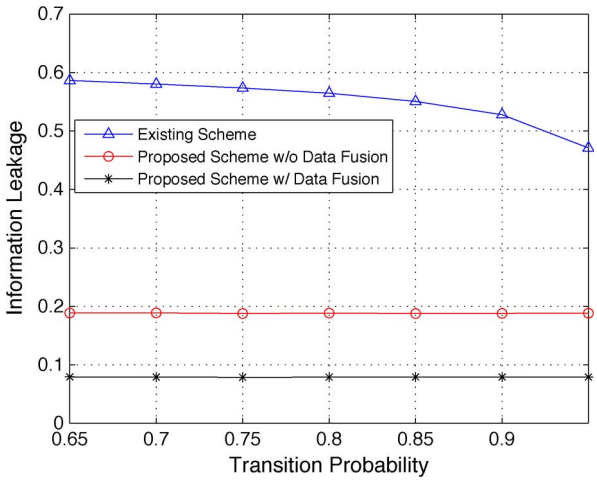

Fig. 6. Information leakage comparison among three schemes under different transition probabilities.

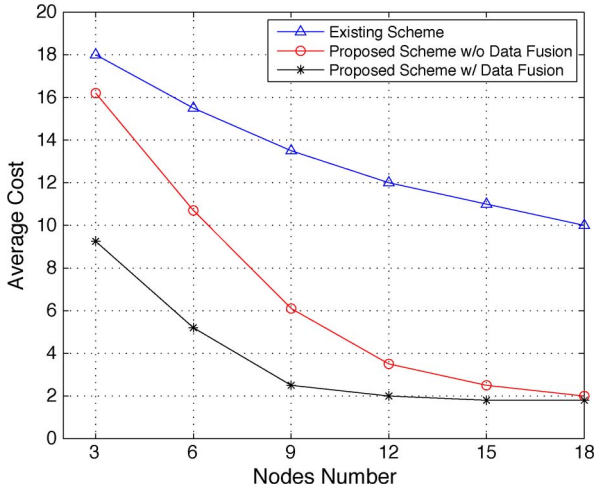

Fig. 7. Cost comparison among three schemes with varying nodes in the network.

number of available nodes in the network increases from 3 to 18. The reason is that there are more nodes that can be selected for authentication and intrusion detection, and therefore, compromised nodes or low-energy nodes can be avoided. When the number of nodes increases to a certain level, where most of the nodes are in secure states, the average cost of the proposed schemes approaches the same low value.

B. 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. Fig. 8 shows the average network compromised probability within the first 40 steps when the first component in the security transition probability matrix of the IDS varies from 0.65 to 0.95 and all other probability values remain constant. Results

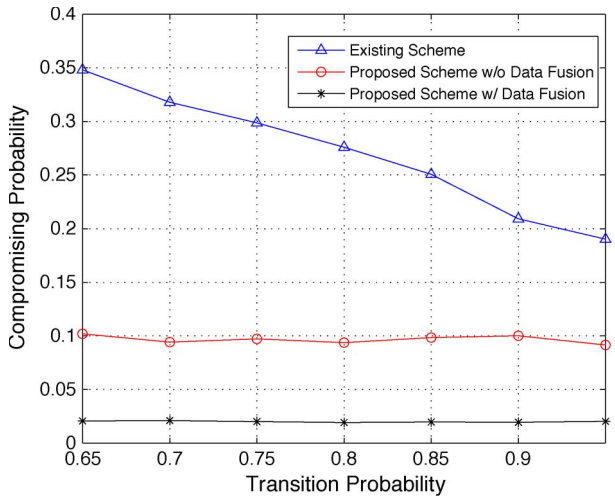

Fig. 8. Network compromise comparison among three schemes under different transition probabilities.

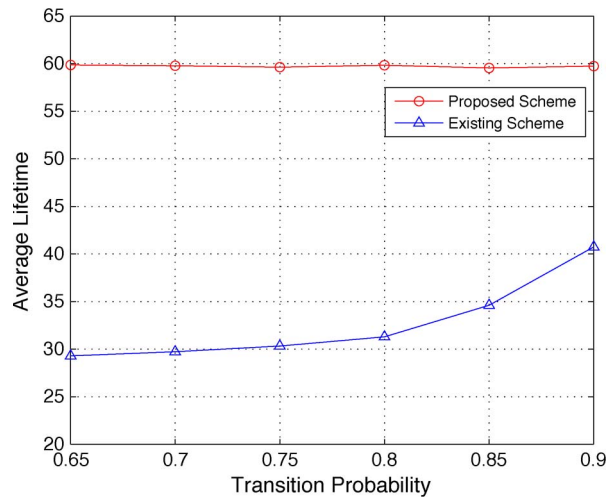

Fig. 9. Network lifetime comparison between the proposed scheme and the existing scheme under different energy transition probabilities.

show that the network compromise probability of two proposed schemes remains low and stable. When the security transition probability is low, meaning that the IDS is easily compromised, the proposed schemes outperform the existing scheme by an even greater amount than the case when the IDS is more secure. The reason is that the proposed schemes avoid choosing the compromised nodes, therefore decreasing the probability of the whole network becoming compromised.

C. 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.

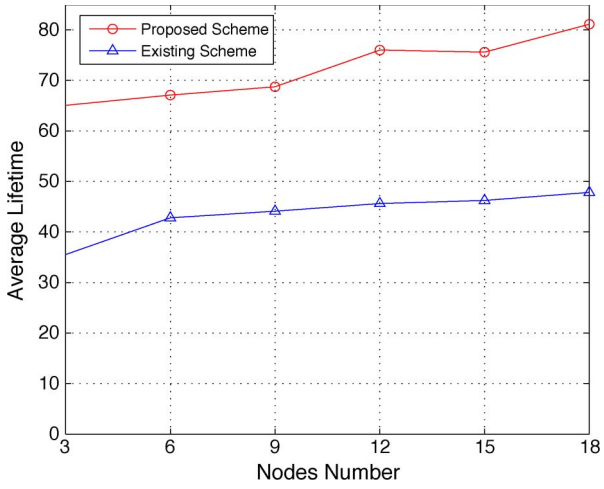

Fig. 10. Network average lifetime with varying number of nodes.

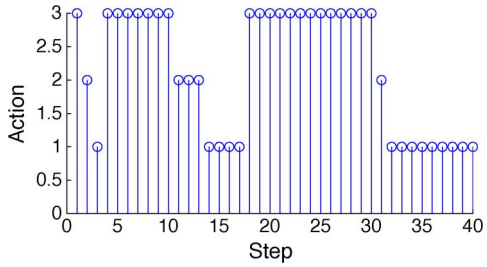

Fig. 11. Example of the policy derived from the proposed scheme without data fusion. (Action = 1: The iris sensor is selected; Action = 2: The fingerprint sensor is selected; Action = 3: The IDS is selected).

We first check the performance when different energy transition probabilities are used. In the simulations, the first element in the energy state transition probability matrix of the IDS varies from 0.65 to 0.9, and all other probability values remain constant. Fig. 9 shows that the proposed scheme has longer network lifetime than the existing scheme since the proposed scheme selects the nodes based on their energy states and only selects the expensive energy-consuming sensors when necessary. Hence, in the proposed scheme, the energy can be more efficiently used. In addition, as we can see from Fig. 9, the average network lifetime in the existing scheme is increased when the energy transition probability is increased because when the energy transition probability is increased, it is more likely that the system stays in a high-energy state. The results also show that the network lifetime of the proposed scheme remains high and stable. The network lifetime is also compared in Fig. 10, showing that the network lifetime increases with the total number of nodes, and the proposed scheme shows significant improvement over the existing scheme. The proposed scheme provides longer network lifetime through optimal scheduling.

Fig. 11 shows an example of the policy for optimal scheduling in the proposed scheme without data fusion. We can see that different sensors, iris, fingerprint, or IDS are dynamically scheduled as the simulation runs to minimize the information leakage and maximize MANET's network lifetime.

VI. 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 have presented 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.

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.

Acknowledgment

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped to improve the quality of this paper.

References

[1] 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.

[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] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," in *Proc. Workshop Multimodal User Authentication*, Santa Barbara, CA, Dec. 2003.

[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] 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.
[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] 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.
[14] C. Katar, "Combining multiple techniques for intrusion detection," *IJCSNS Int. J. Comput. Sci. Netw. Security*, vol. 6, no. 2B, pp. 208–218, Feb. 2006.
[15] P. Hu, Z. Zhou, Q. Liu, and F. Li, "The HMM-based modeling for the energy level prediction in wireless sensor networks," in *Proc. IEEE Conf. Ind. Electron. Appl.*, Harbin, China, May 2007, pp. 2253–2258.
[16] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.—Special Issue on Biometrics*, vol. 2008, no. 113, pp. 1–17, Jan. 2008.
[17] P. Whittle, "Multi-armed bandits and the Gittins index," *J. R. Stat. Soc. Ser. B*, vol. 42, no. 2, pp. 143–149, 1980.
[18] J. Gittins, *Multi-Armed Bandit Allocation Indices*. Hoboken, NJ: Wiley, 1989.
[19] D. Ruta and B. Gabrys, "An overview of classifier fusion methods," *Comput. Inf. Syst.*, vol. 7, pp. 1–10, 2000.
[20] 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.
[21] V. Krishnamurthy and R. J. Evans, "Hidden Markov model multiarmed-bandits: A methodology for beam scheduling in multitarget tracking," *IEEE Trans. Signal Process.*, vol. 49, no. 12, pp. 2893–2908, Dec. 2001.
[22] A. R. Cassandra, "Exact and approximate algorithms for partially observed Markov decision process," Ph.D. dissertation, Brown Univ., Providence, RI, 1998.
[23] V. Krishnamurthy, "Emission management for low probability intercept sensors in network centric warfare," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 41, no. 1, pp. 133–151, Jan. 2005.
[24] 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.
[25] A. R. Cassandra, [accessed Apr. 5, 2010]. [Online]. Available: http://www.cassandra.org/pomdp/code/index.shtml/
[26] 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.
[27] Y. Liang and V. Veeravalli, "Capacity of noncoherent time-selective block Rayleigh flat-fading channel," in *Proc. IEEE Symp. Inf. Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 166.

Shengrong Bu (S'10) received the B.Eng. degree in mechanical and automation engineering from Huazhong University of Science and Technology, Wuhan, China, in 2000 and the M.Eng. degree by research in electrical engineering from the University of Wollongong, Wollongong, Australia, in 2005. She is working toward the Ph.D. degree with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada.

Her research interests include mobile ad hoc networks, wireless network security, green communications, smart grid, and stochastic optimization.

F. Richard Yu (S'00–M'04–SM'08) received the Ph.D. degree in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 2003.

From 2002 to 2004, he was with Ericsson, Lund, Sweden, where he worked on the research and development of Third-Generation cellular networks. From 2005 to 2006, he was with a start-up in California, where he worked on research and development in the areas of advanced wireless communication technologies and new standards. He joined Carleton School of Information Technology and the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, in 2007, where he is currently an Assistant Professor. He serves on the editorial boards of several journals, including the *EURASIP Journal on Wireless Communications Networking*, *Ad Hoc & Sensor Wireless Networks*, the *Wiley Journal on Security and Communication Networks*, and the *International Journal of Wireless Communications and Networking*. His research interests include cross-layer design, security, and quality-of-service provisioning in wireless networks.

Dr. Yu serves on the editorial board of the IEEE COMMUNICATIONS SURVEYS & TUTORIALS. He has served on the Technical Program Committee (TPC) of numerous conferences and as Publication Chair of the 2010 International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Co-Chair of the 2009 ICUMT International Workshop on Cognitive Wireless Communications and Networking, and TPC Co-Chair of the 2011 IEEE Global Communications Conference, the 2011 INFOCOM Workshop on Green Communications and Networking, the 2010 INFOCOM Workshop on Cognitive Wireless Communications and Networking, the 2009 IEEE International Wireless Communications and Mobile Computing Conference, the IEEE Vehicular Technology Conference 2008F Track 4, and the 2007 International Workshop on Wireless Networking for Intelligent Transportation Systems. He was the recipient of the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009 and Best Paper Awards at the 2009 IEEE/IFIP TrustCom and the 2005 International Conference on Networking.

Xiaoping P. Liu (SM'10) received the B.Sc. and M.Sc. degrees from Northern Jiaotong University, Beijing, China, in 1992 and 1995, respectively, and the Ph.D. degree from the University of Alberta, Calgary, AB, Canada, in 2002.

Since July 2002, he has been with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, where he is currently a Canada Research Chair Professor. He serves as an Associate Editor for several journals, including the *Intelligent Service Robotics*, the *International Journal of Robotics and Automation*, *Control and Intelligent Systems*, and the *International Journal of Advanced Media and Communication*. He has published more than 150 research articles. His research interests include interactive networked systems and teleoperation, haptics, micromanipulation, robotics, intelligent systems, context-aware intelligent networks, and their applications to biomedical engineering.

Dr. Liu is a Professional Engineer of Ontario (P.Eng.). He serves as an Associate Editor for several journals, including the IEEE/ASME TRANSACTIONS ON MECHATRONICS and the IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING. He has served on the Organization Committees of numerous conferences, including being the General Chair of the 2008 IEEE International Workshop on Haptic Audio Visual Environments and their Applications and the General Chair of the 2005 IEEE International Conference on Mechatronics and Automation. He was the recipient of the 2007 Carleton Research Achievement Award, the 2006 Province of Ontario Early Researcher Award, the 2006 Carty Research Fellowship, the Best Conference Paper Award of the 2006 IEEE International Conference on Mechatronics and Automation, and the 2003 Province of Ontario Distinguished Researcher Award.

Peter Mason received the B.Sc. degree in mathematics and the M.Sc. and Ph.D. degrees in physics.

He is a Scientist and Leader of the Secure Mobile Networking Group with the Defence Research and Development Canada (DRDC), Ottawa, ON, Canada. He heads a five-year research project funded by DRDC focusing on the security of mobile ad hoc networks. He is also an Adjunct Professor with the University of Ottawa and the University of Ontario Institute of Technology, Oshawa, ON, where he is the supervisor of several graduate students.

Helen Tang (M'07) received the Ph.D. degree from Carleton University, Ottawa, ON, Canada, in 2005.

From 1999 to 2005, she worked in a few R&D organizations in Canada and in the United States, including Alcatel-Lucent, Mentor Graphics, and the Communications Research Center Canada. Since October 2005, she has been with the Network Information Operations Section, Defence Research and Development Canada, Ottawa, as a Defence Scientist. She has published more than 20 research papers in international journals and conference proceedings, including the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the *Journal of Security and Communication Networks*, and the Proceedings of the IEEE International Conference on Communications, the IEEE Vehicular Technology Conference, the IEEE Military Communications Conference, and the IEEE Global Communications Conference (Globecom). Her research interests include ad hoc and sensor networks, wireless network security, communication protocols, and performance analysis.

Dr. Tang has served as Reviewer, Session Chair, and technical committee member for various conferences.