

Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks

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

Abstract—Continuous user authentication is an important prevention-based approach to protect high security mobile ad-hoc networks (MANETs). On the other hand, intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities. Considering these two approaches jointly is effective in optimal security design taking into account system security requirements and resource constraints in MANETs. To obtain the optimal scheme of combining continuous user authentication and IDSs in a distributed manner, we formulate the problem as a partially observable Markov decision process (POMDP) multi-armed bandit problem. We present a structural results method to solve the problem for a large network with a variety of nodes. The policies derived from structural results are easy to implement in practical MANETs. Simulation results are presented to show the effectiveness and the performance of the proposed scheme.

Index Terms—Authentication, intrusion detection, mobile ad-hoc networks, security.

I. INTRODUCTION

WITH recent advances in mobile computing and wireless communications, mobile ad-hoc networks (MANETs) are becoming more attractive for use in various applications [1]. Security issue is an important issue for mobile ad hoc networks, especially for those security-sensitive applications. Two classes of approaches, prevention-based (such as user authentication) and detection-based (such as intrusion detection), can be used to protect high security MANETs. User authentication is critical in preventing non-authorized users from accessing or modifying network resources in high security MANETs. User authentication needs to be performed continuously and frequently, since the chance of a device in a hostile environment being captured is extremely high [2]. Biometrics technology, such as the recognition of fingerprints,

irises, retinas, etc., provides some possible solutions to the continuous user authentication problem in MANETs [3], since it has direct connection with user identity. Intrusion detection systems (IDSs) are also important in high security MANETs to effectively identify malicious activities. In the MANETs, host-based IDSs are suitable since no centralized gateway or router exists in the networks [4].

Many efforts have been made to research on either continuous user authentications or host-based intrusion detection systems. Authors of [2] presented the theory, architecture, implementation, and performance of a multimodal biometrics verification system, and also proposed new metrics against which they benchmark their system. A biometric method for continuous user authentication using a fuzzy controller was presented in [5]. Authors of [6] proposed a data pre-processing method to improve a hidden Markov model (HMM) training for host-based anomaly intrusion detection. A mobile battery-based intrusion detection (B-BID) method was presented in [7] to correlate attack activities with device power consumption patterns. Chari *et al.* [8] presented their experiences with building BlueBox, a policy-driven host-based intrusion detection system.

Continuous authentication and intrusion detection can be considered jointly to further improve the performance of high security MANETs. However, little research has been done in combining these two classes of approaches in MANETs. The authors in [9] proposed a useful framework to combine user authentication and intrusion detection. However, the proposed scheme in [9] is a centralized scheme, in which the whole network is formulated as a single partially observable Markov decision process (POMDP). Solving the POMDP can be computationally intractable since the state space of the POMDP grows exponentially with the number of biometric sensors and IDSs [10]. Therefore, new schemes have to be proposed for a MANET with a large number of distributed nodes.

In this paper, we present a fully distributed scheme of combining continuous authentication and intrusion detection in high security MANETs. A user authentication (or IDS) can be scheduled in a distributed manner considering both the security situations and resources (e.g., node energy) in MANETs. The distributed continuous user authentication and intrusion detection scheduling problem is formulated as a POMDP multi-armed bandit problem. We present a structural results method for solving the scheduling problem in a large network with a variety of nodes. We show that, under reason-

Manuscript received November 26, 2010; revised March 8, 2011; accepted April 25, 2011. The associate editor coordinating the review of this paper and approving it for publication was Z. Han.

This work is supported by the Natural Science and Engineering Research Council of Canada. This work was supported by the Natural Sciences and Engineering Research Council (NSERC) and industrial and government partners, through the Healthcare Support through Information Technology Enhancements (hSITE) Strategic Research Network.

S. Bu, F. R. Yu, and X. P. Liu are with the Department of Systems and Computer Engineering, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6 (e-mail: {shengrbu, pliu}@sce.carleton.ca, richard_yu@carleton.ca).

H. Tang is with Defense R&D Canada, Ottawa, ON, Canada (e-mail: helen.tang@drdc-rddc.gc.ca).

Digital Object Identifier 10.1109/TWC.2011.071411.102123

able conditions on MANETs, structural results can be derived for the combined continuous user authentication and intrusion detection problem, which are trivial to implement and make the solution practically useful. Simulation results are presented to show the effectiveness and the performance of the proposed scheme.

The rest of the paper is organized as follows. Section II introduces the proposed scheme for user authentication and intrusion detection in MANETs, and also formulates the system. Section III shows the solution to the problem. Section IV discusses the computational complexity and communication overhead. Section V presents the simulation results. Finally, we conclude this study in Section VI.

II. MULTIMODEL BIOMETRIC-BASED CONTINUOUS USER AUTHENTICATION AND INTRUSION DETECTION

Most authentication systems do not need to re-authenticate the users for continuous access to the protected resources. However, in hostile environments where the chances of a node being captured are high, user authentication is needed not only for the initial login, but also to verify the presence of the authentic user continuously, in order to reduce the vulnerability of the system [9]. The frequency depends on the situation severity and the resource constraints of the network. Using biometrics technology, individuals can be automatically and continuously identified or verified by their physiological or behavioral characteristics without user interruption [3], [11]. Multimodel biometrics can further improve the security performance of the MANETs by utilizing advantages of various biometrics in different situations.

A. MANETs Equipped with Biosensors and IDSs

Assume that a MANET has a biometric-based continuous authentication system with $N - D$ biosensors and D IDSs, which have the ability to detect intrusions. The IDSs are also modeled as sensors bringing the total number of sensors to N . In the rest of this paper, we use *sensor* to refer to an authentication device or an intrusion detection device. Without loss of generality, we assume that some nodes have one or more biosensors, and some do not have any 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 is illustrated in Fig. 1.

The system can perform two kinds of operations: intrusion detection and 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. Biometric information transmitted between biometric sensors and their remote storage entity with biometric templates [12] may be detected by adversaries, who can break into the biometric systems by performing various attacks (e.g., a replay attack) [13]. Therefore, performing authentication and intrusion detection may lead to security information leakage

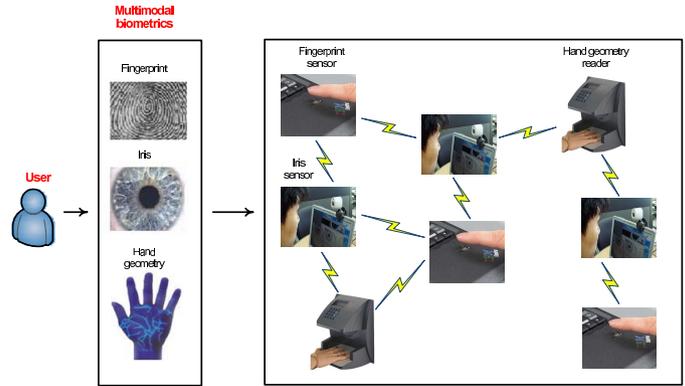


Fig. 1. An example framework for a MANET with multimodal biometrics.

to an adversary monitoring communications and network behavior. It is critical for the system to optimally schedule the intrusion detection and continuous authentication activities for each time slot in a distributed manner, taking system security and resource (e.g., node energy) into account.

In biometric authentication and IDS processes, false acceptance (FA) and false negative (FN) errors can result in security breaches, since unauthorized persons are admitted to access the system/network or intrusions are not detected and therefore no alert is raised. The security state of the system may not be observed perfectly due to these errors. Therefore, we formulate the distributed user authentication and intrusion detection scheduling problem as a stochastic partially observed Markov decision process (POMDP) multi-armed bandit problem [10], [14], which is a powerful framework to solve the distributed optimization problem.

B. System Model

We consider that the time axis is divided into equal time slots, which correspond to the time intervals between two continuous user authentications or intrusion detection. Let the state of a *sensor* (biometric sensor or IDS) $n, n \in \{1, 2, \dots, N\}$, be $x_k^{(n)} = (s_k^{(n)}, e_k^{(n)})$ at time slot k , which includes the sensor security state $s_k^{(n)}$ and energy state $e_k^{(n)}$. The security condition of each sensor can be divided into L discrete levels, such as $\{secure, attacked, compromised\}$. The security state space \mathcal{S} includes all the security states $\{s_1, \dots, s_L\}$. The residual battery energy of each sensor can be divided into Q discrete levels, such as $\{low_energy, middle_energy, high_energy\}$. The residual energy state space \mathcal{E} includes all the energy states $\{e_1, \dots, e_Q\}$. The states $s_k^{(n)}$ and $e_k^{(n)}$ evolve based on L -state and Q -state Markov chains with state transition probability matrix $U^{(n)}$ and $W^{(n)}$, respectively, if sensor n is used at time k , which are described as follows:

$$U^{(n)} = \left(s_{ij}^{(n)} \right)_{i,j \in \mathcal{S}}, \text{ where } s_{ij}^{(n)} = P \left(s_{k+1}^{(n)} = j | s_k^{(n)} = i \right).$$

$$W^{(n)} = \left(e_{ij}^{(n)} \right)_{i,j \in \mathcal{E}}, \text{ where } e_{ij}^{(n)} = P \left(e_{k+1}^{(n)} = j | e_k^{(n)} = i \right).$$

If sensor n is idle at time k , the state of this idle sensor, $x_k^{(n)} = (s_k^{(n)}, e_k^{(n)})$ is unchanged, i.e., $s_{k+1}^{(n)} = s_k^{(n)}$ and $e_{k+1}^{(n)} = e_k^{(n)}$.

Let $\mathcal{X}^{(n)}$ with X_n states be sensor n 's state space. The state transition probability matrix $T^{(n)}$ can be computed based on $U^{(n)}$ and $W^{(n)}$.

In practical MANETs, the state of the chosen sensor n may not be observed directly. The observation of its state, $y_k^{(n)} = (y_{s,k}^{(n)}, y_{e,k}^{(n)})$, includes the observation of its security state $y_{s,k}^{(n)}$ and the observation of its energy state $y_{e,k}^{(n)}$ at time slot k . Let $\mathcal{Y}^{(n)}$ with Y_n states be the observation state space. If sensor n is picked at time slot k and the security state $s_k^{(n)}$ equals to i , the probability of obtaining security observation m is denoted as:

$$b_i(a_k = n, y_{s,k}^{(n)} = m) = P(y_{s,k}^{(n)} = m | s_k^{(n)} = i, a_k = n), \quad (1)$$

where $i \in \mathcal{S}$, and $m \in \mathcal{M}$, and \mathcal{M} is the state space of observations of the security state. Define the observation matrix of selected sensor n 's security state as:

$$B_s^{(n)}(y_{s,k}^{(n)} = m) = \text{diag}[b_1(n, m), \dots, b_L(n, m)]. \quad (2)$$

The observation matrix of selected sensor n 's energy state $B_e^{(n)}$ can be also defined using the above method. Matrix $B^{(n)}$ denotes the probability of the observation $y_k^{(n)}$ when sensor n is picked at time slot k , which can be computed based on matrix $B_s^{(n)}$ and matrix $B_e^{(n)}$.

Security-related and energy-related costs are considered in our scheme, since transmitted biometric information may be detected by adversaries, and energy is certainly consumed when a sensor is used. Let $a_k \in \{1, \dots, N\}$ denote the 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, which $c(x_k^{(n)}, n) = (1 - \lambda)c_s(s_k^{(n)}, n) + \lambda c_e(e_k^{(n)}, n)$, where $\lambda \in (0, 1)$ is the weight factor for these two kinds of costs. β ($0 \leq \beta < 1$) denotes the discount factor, which can model the fact that future cost is worth less than immediate cost because the future is less certain. The weight factor can be set differently in different applications. For example, in a battlefield MANET, the weight factor λ can be set to a value close to 0, which reflects the fact that information leakage is more important than energy loss in the battlefield network. By contrast, in a civilian MANET, λ can be set to a larger value, which reflects the fact that energy loss is more important than information leakage in the civilian network.

Denote the observation and action (sensor selection) history at time k as $Y_k \triangleq (y_1^{(a_0)}, \dots, y_k^{(a_{k-1})})$ and $A_{k-1} \triangleq (a_0, \dots, a_{k-1})$, respectively. One sensor is chosen at time $k+1$ according to $a_{k+1} = \mu(Y_{k+1}, A_k)$, where the policy denoted as μ belongs to the class of stationary policy η . The total expected discounted cost over an infinite-time horizon is given by

$$J_\mu = E \left[\sum_{k=0}^{\infty} \beta^k \left(c(x_k^{(a_k)}, a_k) \right) \right]. \quad (3)$$

The optimization objective is to find the optimal stationary policy $\mu^* = \arg \min_{\mu \in \eta} J_\mu$ to minimize the cost in (3).

III. STRUCTURAL RESULTS METHOD FOR COMBINING CONTINUOUS AUTHENTICATION AND INTRUSION DETECTION

The decision about which sensor is chosen at each time slot should depend on all the actions and observations history, since the sensors' states are only partially observable. To this end, *information state* is developed to derive sufficient statistical information for the past history. The information state $\pi_k^{(n)}$ of sensor n at time slot k refers to a probability distribution over the sensor's states. Its entire probability space (the set of all possible probability distributions) is referred to as the information state space $\Psi^{(n)}$, which is totally observable. If a sensor is chosen, its information state at that time can be updated using the hidden Markov model state filter with the new observation. Otherwise, their information states remain unchanged at that time slot. Therefore, the above POMDP multi-armed bandit problem can be re-expressed as a fully observable multi-armed bandit problem in terms of the information state, which means the optimal sensor can be chosen based on the information state [15].

A. Gittins Index Policy

For our proposed scheme, the optimal policy has an *indexable rule*, meaning that the optimal policy can be found according to the Gittins indices of the sensors $\gamma^{(n)}(\pi_k^{(n)})$ ($n = 1, \dots, N$) [15]. The Gittins index of a sensor is a function of that sensor's characteristics (e.g., state transition probabilities) and its information state. The optimal policy at time k is that the sensor with the largest reward Gittins index at that time should be selected when the reward is the optimization objective, which significantly decreases the computational complexity compared to using the POMDP methods [10].

One common method for computing the Gittins index of each sensor is a value iteration algorithm [10]. However, the value iteration-based solution for computing the Gittins index only works for a MANET with a small number of nodes and a small number of states and observation states. For a large network with a variety of nodes, the value iteration-based solution can become computationally intractable [10], illustrated in Table I.

B. Monotone Gittins Index in the Structural Results Method

In this section, we show that, under reasonable conditions on the cost vector C , state transition probability matrix T and observation probability matrix B of each node in MANETs, the Gittins index in our problem can be monotone increasing in the information state (with respect to the monotone likelihood ratio (MLR) ordering [10]). This means that if the information states of these N sensors at a given time instant are MLR comparable, the optimal policy is to pick the authentication sensor or the intrusion detection system with the smallest information state with respect to the MLR ordering. Namely, the sensor with the higher probability of being in the better state has a higher possibility of being chosen at that time slot,

if the information states are MLR comparable. The definition of MLR ordering used in this paper is described as follows.

Definition 3.1: MLR Ordering.

Assume that each sensor includes the same number of security and energy levels. Namely, X_1, \dots, X_N are equal to X .

- 1) Let π_1 and π_2 be two information state vectors. Then, π_1 is less than π_2 with respect to the MLR ordering – denoted as $\pi_1 \leq_r \pi_2$ if $\pi_1(i)\pi_2(j) \geq \pi_2(i)\pi_1(j)$, $i < j$, $i, j \in \{1, \dots, X\}$. For example, $\pi_1 = [0.3 \ 0.2 \ 0.5]$ and $\pi_2 = [0.1 \ 0.2 \ 0.7]$, then $\pi_1 \leq_r \pi_2$.
- 2) A function $f(\cdot)$ is MLR increasing if for all $\pi_1, \pi_2 \in \Psi$, $\pi_1 \leq_r \pi_2$ implies $f(\pi_1) \leq f(\pi_2)$.
- 3) Let $\pi^{(1)}, \pi^{(2)}, \dots, \pi^{(N)}$ denote the information states of N sensors. Then they are said to be MLR comparable if for any $n, \tilde{n} \in \{1, \dots, N\}$, either $\pi^{(n)} \leq_r \pi^{(\tilde{n})}$ or $\pi^{(n)} \geq_r \pi^{(\tilde{n})}$.
- 4) Given MLR comparable information states of these N sensors, denote the smallest information state (with respect to MLR ordering) as $\min\{\pi^{(1)}, \dots, \pi^{(N)}\}$ with index $\arg \min\{\pi^{(1)}, \dots, \pi^{(N)}\}$.

In the following, we present the conditions on the parameters C , T and B of an arbitrary sensor, where its Gittins index $\gamma(\pi)$ is monotone in information state π with respect to the MLR ordering.

Theorem 1: Consider the following assumptions for each sensor:

Assumption 1: Costs satisfy $C(i) \leq C(i+1)$.

Assumption 2: State transition probability matrix T is totally positive of order 2 (TP2), i.e., all its second order minors are non-negative. That is, determinants

$$\begin{vmatrix} t_{i_1 j_1} & t_{i_1 j_2} \\ t_{i_2 j_1} & t_{i_2 j_2} \end{vmatrix} \geq 0 \text{ for } i_2 \geq i_1, j_2 \geq j_1.$$

Assumption 3: Symbol probabilities satisfy $(b_{i,m})_{m \in M} \leq_r (b_{i+1,m})_{m \in M}$ for $i = 1, \dots, X-1$.

Then the Gittins index $\gamma(\pi)$ of each sensor is MLR increasing. Therefore, if the information states of the N sensors are MLR comparable, then the optimal policy μ^* is to pick the sensor with the smallest information state with respect to MLR ordering at each time slot, namely, $a_k = \mu^*(\pi_k^{(1)}, \dots, \pi_k^{(N)}) = \arg \min(\pi_k^{(n)})$, $n \in \{1, \dots, N\}$.

The above theorem says that if the information states of the sensors are MLR comparable, then the optimal policy is a greedy policy. We give the following examples to explain the optimal policies in different scenarios. In a battlefield MANET, assume that information leakage is far more important than energy loss. In this case, we can consider two states, {secure, compromised}, for each sensor, and all information states are MLR comparable. The optimal policy in this case is to choose the sensor with a higher probability of being in the secure state at each time slot. Similarly, in a civilian MANET, where energy loss is more important than information leakage, we can consider two states, {high-energy, low-energy}, for each sensor, and all information states are MLR comparable. The optimal policy in this case is to choose the sensor with a higher probability of being the high-energy state at each time slot. In Section VII, Simulation Results and Discussions, we

have added some simulation results in Figs. 6 and 9 about battlefield MANETs and civilian MANETs.

In the following, we show that, under reasonable conditions on the matrices of each node in MANETs, the distributed continuous user authentication and intrusion detection system meets the above three assumptions. Assumption 1 shows that for an arbitrary sensor, the cost in state i is less than or equal to that in state $i+1$. In the distributed continuous user authentication and intrusion detection scheduling problem, the cost vector of each sensor always meets this assumption, since there is more information leakage when a chosen node is in a more dangerous state than when it is in a safer state. Therefore, the cost of selecting a node in the more secure and higher energy state is lower than that of selecting a more compromised and lower energy node.

Assumption 2 holds in the following situation. Due to continuity arguments, if the state of a sensor is x_i , $1 \leq i \leq X$ at time k , then at time $k+1$, it is reasonable to assume that it is either still in state x_i , or, with a lower probability, in the neighboring states x_{i+1} or x_{i-1} . Therefore, in our proposed scheme, each sensor can be modeled as a X -state Markov chain with diagonally dominant tridiagonal transition probability matrix T , where $t_{ij} = 0$ for $j \geq i+2$ and $j \leq i-2$. The following matrix is an example of a diagonally dominant tridiagonal matrix.

$$\begin{pmatrix} 0.9 & 0.1 & 0 & 0 \\ 0.1 & 0.8 & 0.1 & 0 \\ 0 & 0.1 & 0.8 & 0.1 \\ 0 & 0 & 0.1 & 0.9 \end{pmatrix}.$$

According to [16], a necessary and sufficient condition for tridiagonal matrix T to meet Assumption 2 is that $t_{i,i}t_{i+1,i+1} \geq t_{i,i+1}t_{i+1,i}$.

Several common observation probability models for MANETs that satisfy Assumption 3 are listed as follows:

- 1) Each sensor measures the target in quantized Gaussian noise.
- 2) Observation probabilities die geometrically fast with the error between the reported observation y and the real state x .
- 3) The value the sensor reports is never more than one discrete value away from the true value. Therefore, B matrix is the following $X \times X$ tridiagonal matrix:

$$\begin{pmatrix} \frac{p_1}{2} & 1-p_1 & 0 & 0 & \dots \\ 0 & \frac{1-p_2}{2} & p_3 & \frac{1-p_3}{2} & \dots \\ 0 & 0 & 1-p_4 & p_4 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

In the following, we assume that, in our proposed scheme, vector C , matrix T , and matrix B of each sensor meet all of the three assumptions in Theorem 1. The Gittins index $\gamma(\pi)$ is monotone increasing. Therefore, if the information states of the N sensors are MLR comparable, the optimal policy is to pick the authentication or intrusion detection sensor with the smallest information state with respect to MLR ordering.

C. Approximations to the Gittins Index

When there are only 2 states for the N sensors, namely {secure, high_energy}, {compromised, low_energy}, their in-

formation states are always MLR comparable, and the optimal policy will be the same as above. For more states than 2, when the information states are MLR comparable, the optimal policy can be used directly. However, since for ≥ 3 , MLR is a partial ordering, the N information states $\pi^{(1)}, \dots, \pi^{(N)}$ are not necessarily MLR comparable at each time instant. When the trajectories of the information states are not MLR comparable, the following approximations can be used, by projecting the non-MLR comparable information state onto the nearest MLR comparable state.

In the proposed scheme, each sensor starts from the (*secure, high_energy*) state, which means that the information state equal to $(1, 0, \dots, 0)$, where all elements equal to zero, except the first. Therefore, the information states of all N sensors are identical. Assume at time instant k , the information states of all N sensors are MLR comparable. Let $\sigma(1), \dots, \sigma(N)$ denote the permutation of $(1, \dots, N)$, so that $\pi_k^{\sigma(1)} \leq_r \pi_k^{\sigma(2)} \leq_r \dots \leq_r \pi_k^{\sigma(N)}$. From the above theorem, the optimal action is $a_k = \sigma(1)$. But at the time $k + 1$, the updated information state $\pi_{k+1}^{\sigma(1)}$ may not be MLR comparable with the other $N - 1$ information states. When the updated information state is not MLR comparable with the other information states, it can be projected to the nearest information state, denoted $\bar{\pi}$, in the simplex Ψ that is MLR comparable with the other $N - 1$ information states. That is, at time $k + 1$, we solve the following N optimization problems:

$$\begin{aligned} G(\bar{\pi}^{(1)}) &= \min_{\bar{\pi} \in \Psi} \|\bar{\pi} - \pi_{k+1}^{\sigma(1)}\| \text{ subject to } \bar{\pi} \leq_r \pi_k^{\sigma(2)} \\ G(\bar{\pi}^{(n)}) &= \min_{\bar{\pi} \in \Psi} \|\bar{\pi} - \pi_{k+1}^{\sigma(n)}\| \text{ subject to} \\ &\quad \pi_k^{\sigma(n)} \leq_r \bar{\pi} \leq_r \pi_k^{\sigma(n+1)}, n = 2, \dots, N - 1 \\ G(\bar{\pi}^{(N)}) &= \min_{\bar{\pi} \in \Psi} \|\bar{\pi} - \pi_{k+1}^{\sigma(N)}\| \text{ subject to } \pi_k^{\sigma(N)} \leq_r \bar{\pi}. \quad (4) \end{aligned}$$

Here, $\|\cdot\|$ denotes some norm, and the 2-norm is used in our simulation. In the equations, G and $\bar{\pi}_n$ denote the minimum value and minimum solution for each equation, respectively. Finally, set $\pi_{k+1}^{\sigma(1)} = \arg \min_{\bar{\pi}_n} G(\bar{\pi}_n)$. The above N problems are straightforwardly shown to be convex optimization problems and can be solved efficiently in real time. Thus, all the information states at time $k + 1$ are now MLR comparable, and the optimal action a_{k+1} is choosing the node with the smallest information state with respect to MLR ordering.

IV. COMPUTATIONAL COMPLEXITY AND COMMUNICATION OVERHEAD

In the centralized scheme [9], the whole network is formulated as a single POMDP, and a centralized controller is needed to schedule authentication and intrusion detection in the whole network. Since the state space of the POMDP in the centralized scheme in [9] grows exponentially with the number of scheduled sensors, solving the POMDP can be computationally intractable [10]. By contrast, 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 distributed scheme is dramatically decreased. The computational complexity can be further reduced in the structural results. The corresponding

simulation results about computational complexity will be presented in Subsection V-A.

In the proposed scheme, communication overhead is mainly due to multicasting the following two types of messages in the real-time scheduling process:

- INITIAL-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 indices.
- SENSOR-INDICES (SIND), 8 bytes, which is sent at the beginning of each time slot by the node active in the previous time slot.

Any network layer multicast algorithm for ad-hoc networks can be used in the scheme.

In the centralized scheme, the centralized controller needs to notify the N sensors from which sensor has been chosen at the beginning of the authentication and intrusion detection process. At each time slot, the active node needs to transmit its observation value to the centralized controller. After that, the controller also needs to notify the nodes of which sensor it has chosen at this time slot. The centralized scheme's total communication overhead is approximately proportional to $4N$ bytes, plus $8 + 4N$ bytes per time slot. The proposed scheme's total communication overhead is proportional to $8N \times (N - 1)$ bytes, plus $8 \times (N - 1)$ bytes per time slot. Therefore, the proposed scheme's communication overhead is greater than that of the centralized scheme.

There are some other tradeoffs within the proposed scheme. For example, in the real-time sensor selection process (mentioned in Section V), each sensor can broadcast the new Gittins index to the other sensors only in certain time slots in order to further decrease the communication overhead. However, the cost becomes higher since the other sensors have to make decision based on out-of-date Gittins indices. In the extreme case, if sensors do not broadcast their Gittins indices to the other sensors at all, sensors have to be chosen randomly at each time slot. The results in Fig. 3 show that the average cost of this random scheme is higher than that in the proposed scheme.

V. SIMULATION RESULTS AND DISCUSSIONS

In this section, we use computer simulations to compare the performance of the centralized scheme and the proposed distributed scheme, and the performance of the two methods used in the proposed scheme. We consider the following simulation scenario. There are two types of biosensors for continuous authentication, iris sensor and fingerprint sensor, and IDSs for intrusion detection. Each sensor has four states: $\{(secure, high-energy), (secure, low-energy), (compromised, high-energy), (compromised, low-energy)\}$. The iris sensor is the most expensive one in terms of energy cost, and also provides the most accurate authentication. The fingerprint sensor provides intermediate accurate authentication, and has intermediate energy cost. IDS uses the least energy, and has the least accuracy in detecting the security state. The following defined matrices are based on the above assumptions. Examples of the state transition probability matrices of the iris sensor,

fingerprint sensor and IDS, when they are active, are defined as follows:

$$T^{(1)} = ((0.912, 0.088, 0.0, 0.0), (0.025, 0.950, 0.025, 0.0), \\ (0.0, 0.044, 0.912, 0.044), (0.0, 0.0, 0.05, 0.95)), \\ T^{(2)} = ((0.784, 0.216, 0.0, 0.0), (0.1, 0.8, 0.1, 0.0), \\ (0.0, 0.059, 0.882, 0.059), (0.0, 0.0, 0.1, 0.9)), \\ T^{(3)} = ((0.9702, 0.0298, 0.0, 0.0), (0.01, 0.98, 0.01, 0.0), \\ (0.0, 0.0149, 0.9702, 0.0149), (0.0, 0.0, 0.02, 0.98)).$$

The observation probability matrix of each node is identical to its state transition probability matrix. The cost vectors are defined as: $C^{(1)} = (3, 8, 20, 40)$, $C^{(2)} = (2, 7, 22, 45)$, $C^{(3)} = (1, 4, 25, 50)$. These specific values are used in all simulations. In the simulations presented in Table I, these matrices were modified to create a variety of similar node types. Since there is more potential for information leakage when a node is in the compromised state than in the secure state, the information leakage cost of selecting a secure node is lower than that of selecting a compromised node¹. The above matrices vary in different applications. For example, the cost value of a sensor in a more compromised state needs to be set much higher than that in a more secure state especially in a battlefield network, so a more secure sensor can be chosen at each time slot. However, in a civilian network, especially for a energy-concerned network, the cost value of a sensor in a lower energy state needs to be set much higher than that in a higher energy state, so a higher energy sensor can be chosen at each time slot.

It is a non-trivial task to setup sensors' state transition probability matrices, observation probability 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 state transition probability matrices, observation probability matrices, and cost matrices. However, in a dynamic environment, where heterogeneous nodes may join the network, it may not be as realistic to assume knowledge of all the sensors' properties. In these circumstances, we should be able to predict and learn the sensors' properties from the history of observations and actions.

We used 'pomdp-solve', a program in C++ from [17], to compute the set of vectors Λ_H . In pomdp-solve, we chose the *incremental pruning algorithm* developed in the artificial intelligence community by Cassandra *et al.* [18], since it is one of the fastest algorithms for solving POMDPs [10]. We implemented the computation of the Gittins indices in Matlab. All simulations are run on a computer equipped with Window 7, Intel Core 2 Duo P8400 CPU (2.26Ghz), 4GB memory. In the simulations, the initial state for each node is (*secure, high-energy*). We adopt the hybrid Manhattan and random waypoint (RWP) mobility model [19] to simulate the node movements.

¹For example, a compromised node could intentionally introduce collisions in a cryptographic protocol.

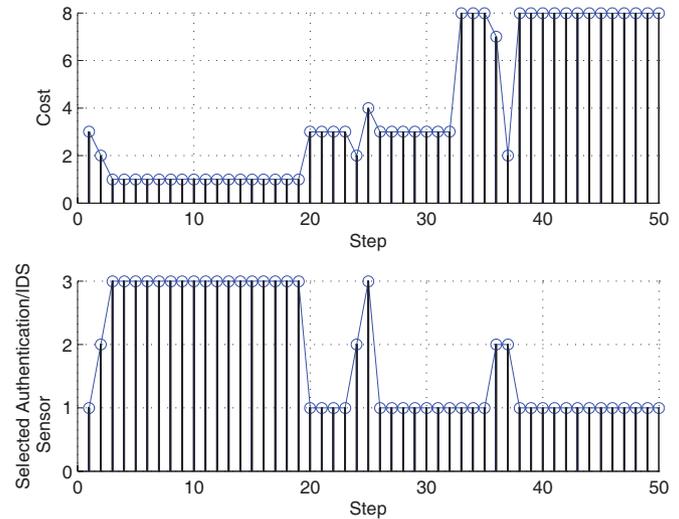


Fig. 2. An example policy derived from the structural results method (1: Iris; 2: Fingerprint; 3: IDS).

Block Rayleigh flat-fading wireless channel model [20] is used in this paper.

A. Computational Efficiency Comparison

Simulations are performed to compare the computational efficiency in the centralized scheme [9] and the proposed distributed scheme. Table I shows the computation time spent in the centralized scheme and the proposed distributed scheme in the off-line and on-line parts, as the total number of node types in the MANET varies from 2 to 50. For the value iteration algorithm, the on-line computation time is of the same level as that of the structural results method. The table also shows that the off-line time is the dominant part for the value iteration algorithm. The computation time dramatically increase when the number of node types changes from 2 to 4: from 0.03 seconds to more than 8 hours. In the structural results method, a *quicksort* algorithm with MLR ordering is used to sort the sensors by current information states. Each value is the averaged result of 1000 simulations. The off-line computation time for the structural results method is always equal to 0, since the method is only used for on-line sensor scheduling. The computation time of the structural results method slightly increase with the increasing type of the nodes in the network. This shows that the structural results are practically useful in real MANETs.

B. Policies Derived from the Structural Results

Fig. 2 shows an example of the policy for optimal scheduling in the proposed scheme using the structural results method. In this example, there are three sensors, one iris, one fingerprint, and one IDS. From Fig. 2, we can see that authentication and IDS are scheduled dynamically as the simulation runs to minimize the information leakage and maximize the network lifetime in the MANET.

We also investigate how the initial states of the sensors affect the MLR non-comparable percentage between the chosen sensor and the idle sensors using the structural results

TABLE I
THE COMPUTATION TIME IN THE CENTRALIZED SCHEME AND THE PROPOSED DISTRIBUTED SCHEME.

Scheme	Method	2 node types	4 node types	20 node types	50 node types
Centralized scheme	Incremental pruning algorithm	2h32m10s	unfeasible	unfeasible	unfeasible
Proposed distributed scheme	Structural results (off-line)	0	0	0	0
	Structural results (on-line)	0.0427s	0.0576s	0.2337s	0.5960s
	Value iteration algorithm (off-line)	0.03s	8h1m22s	unfeasible	unfeasible
	Value iteration algorithm (on-line)	0.0379s	0.0531s	-	-

method, which affects whether or not the structural results method can be directly used in that time slot. Each value is the averaged result of 1000 simulations. Table II shows the percentage of sensor choices in the first 100 steps where the updated information state of the chosen sensor is not MLR comparable, for different choices of initial sensor state. The table shows that the percentage of choices leading to non-MLR-comparable states is near to 0 when the sensors start in the fourth state, since the sensors have a high probability of remaining in the fourth state.

C. Performance Comparison

We perform simulations to compare the performance of the centralized scheme, the random choice scheme and the proposed distributed scheme, and the performance of the two methods used in the proposed scheme. Fig. 3 illustrates the average cost for the first 100 steps of the simulation. Each cost value is the averaged result of 1000 simulations. The figure shows that the average cost of this random scheme is the highest among the three schemes. The figure also shows that the average cost from the proposed distributed scheme is higher than that from the centralized scheme, since the nodes in the centralized scheme can make better decisions as they have complete information. Since the nodes all start from (secure, high-energy), the average costs using of different schemes all begin at a low level, and diverge as over time as the network changes states. The results show that the average cost from the value iteration algorithm and that from the structural results method are very close to each other. Fig. 4 illustrates the relative information leakage, which is defined as the information leakage of the selected node divided by the information leakage when the node is in the worst state. The same observation is true with the information leakage in Fig. 4. This shows the effectiveness of these two methods, both of which can provide optimal policies that minimize the information leakage and maximize the network lifetime. The reasons why the result from the value iteration algorithm is not exactly the same as that from the structural results method are as follows:

- 1) For the value iteration algorithm, the finite-horizon Gittins index approximation can be made arbitrarily accurate by choosing a sufficiently large horizon H , which is a tradeoff between performance and computation time.
- 2) For the structural results method, the updated information state of the chosen sensor has to project to the nearest MLR comparable information state when the updated information state is not MLR comparable to those of the other sensors, therefore some errors are generated. Nevertheless, the errors are small, which

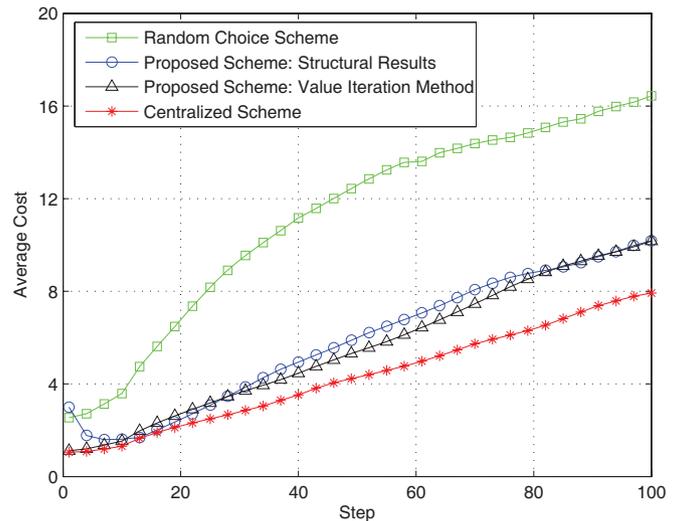


Fig. 3. Average cost comparison of the centralized scheme, the random choice scheme, and the proposed distributed scheme.

make the results from the structural results method are very close to those from the value iteration algorithm.

Figs. 3 and 4 also show that the results from the two methods are quite different in the early steps. The reason is that the sensors all start in the first state, which means their information states are $(1, 0, 0, 0)$. Therefore, they are identical, and one of the sensors is chosen randomly in the structural results method. However, for the value iteration algorithm, the sensor that can minimize the total expected discounted cost is chosen at each time slot. After about 10 steps, the results are very close in these two methods.

Different numbers of nodes are also used in the simulations to verify the scalability of the proposed scheme using each method in the battlefield network and civilian network. Fig. 5 and Fig. 6 show the average cost and the average information leakage within the first 100 steps of the simulation of networks of different sizes. In these simulations, we use the same three types of nodes mentioned earlier. The figures show that the average information leakage in the battlefield network is much smaller than that in the civilian network, since the more secure sensors in the battlefield network are the optimal choices rather than the higher-energy ones in the civilian network. The figures show that the average cost and the average information leakage results for the value iteration algorithm and the structural results method in the battlefield network are similar. The results also show that the average cost and the average information leakage decrease when the number of available nodes in the network increases from 3 to

TABLE II
PERCENTAGE OF STATES NOT MLR COMPARABLE IN THE FIRST 100 STEPS.

$\pi_0^{(n)}$	e_1	e_2	e_3	e_4	$\pi_0^{(n)}(i) = 1/4$
Percentage of states not MLR comparable	36.36	99.50	49.01	1.4000e-004	63.25

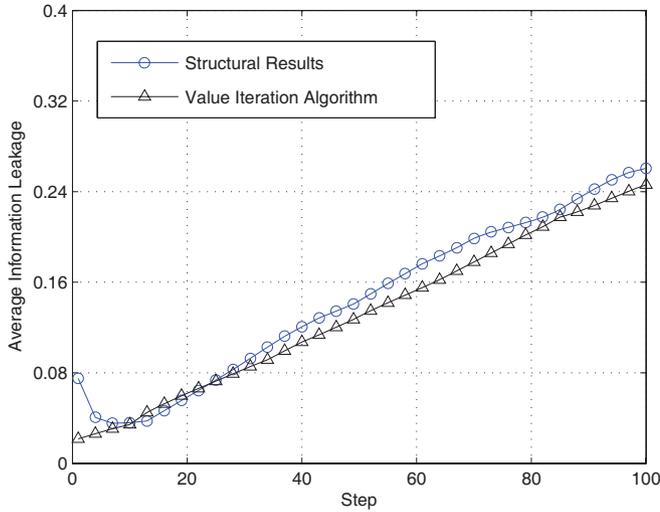


Fig. 4. Average information leakage comparison between the two methods.

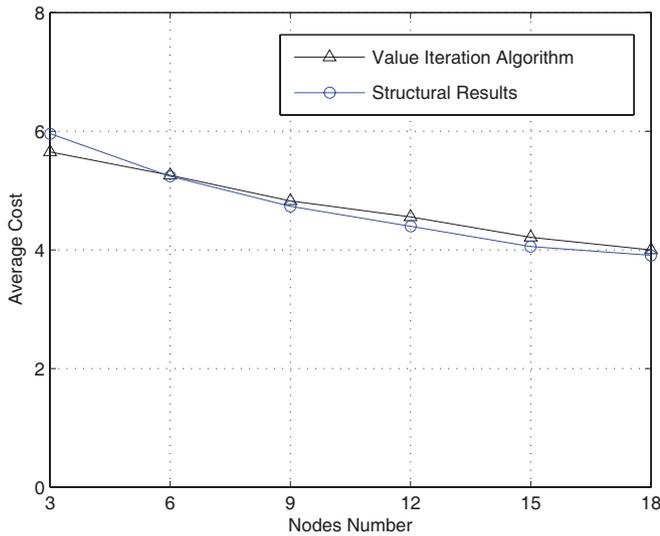


Fig. 5. Average cost comparison between the two methods with different numbers of nodes.

18. The reason is that there are more nodes that can be selected for authentication and intrusion detection, so compromised and low-energy nodes can be avoided.

Various state transition probabilities are also used in the simulations to evaluate the dynamic stability of the proposed scheme using each method. Fig. 7 shows the average cost using these two methods as the first component in the state transition probability matrix varies from 0.7 to 1.0, where high state transition probability means that the system is more secure. The results show that the average costs using these two methods are similar. From Fig. 7, we can observe that the cost decreases when the system becomes more secure. This is

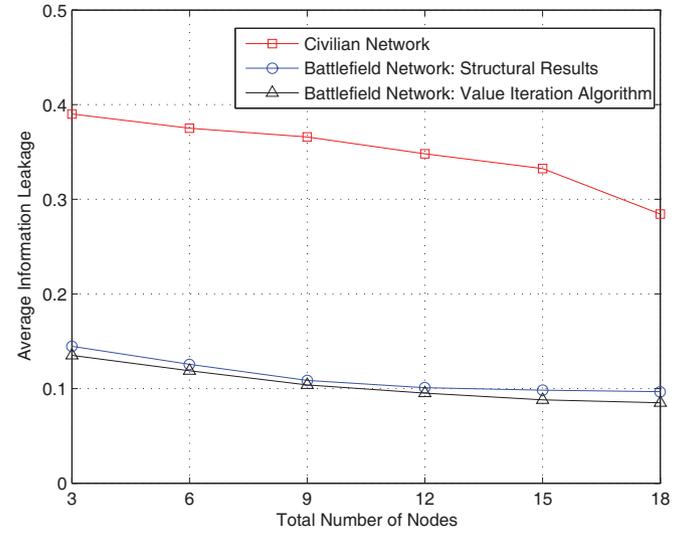


Fig. 6. Average information leakage comparison between civilian network and battlefield network with different numbers of nodes.

because the information leakage is smaller when the system becomes more secure, therefore the cost is smaller. When the state transition probability reaches 1, the average cost of the two methods is quite different. The reason is that when the state transition probability reaches one, the information states do not change, and therefore a sensor is randomly chosen at each time slot. Fig. 8 shows the average information leakage within the first 100 steps when the first component in the state transition probability matrix of the IDS varies from 0.7 to 1.0 and all other probability values remain constant. The average information leakage using these two methods are still close. The results show that information leakage remains stable for the first four probabilities, and decreases when the system becomes more secure. The reason for this is that the proposed schemes avoid choosing the compromised nodes. When the state transition probability further increases, the average information leakage decreases.

D. Network Lifetime Comparison

Network lifetime performance has been evaluated for the proposed scheme using each method, which is illustrated in Fig. 9. In these simulations, the network lifetime is defined as the time until the chosen node is in the low-energy state. The results show that the network lifetime increases with the total number of nodes. The average network lifetime is much higher in the civilian network compared to that of the battlefield network, since the higher-energy sensor is chosen at each time slot, with the tradeoff being greater information leakage. In the battlefield network, the results using the value iteration algorithm and the structural results method are very close.

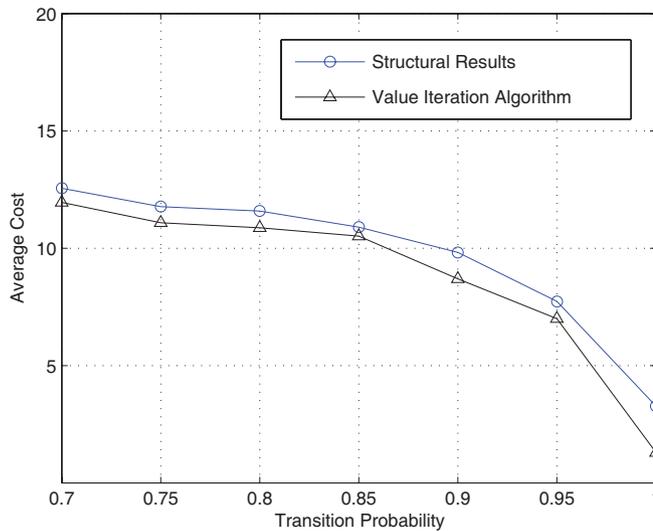


Fig. 7. Average Cost comparison between the two methods with different state transition probabilities.

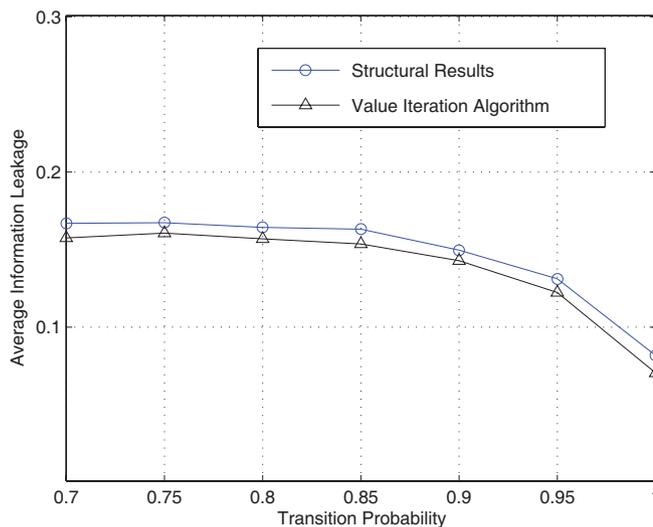


Fig. 8. Average information leakage comparison between the two methods with different state transition probabilities.

VI. CONCLUSIONS AND FUTURE WORK

Combining continuous user authentication and intrusion detection can be an effective approach to improve the security performance in high security MANETs. In this paper, we presented a distributed scheme of combining user authentication and intrusion detection. In the proposed scheme, the most suitable biosensor (for biometric-based authentication) or IDS is dynamically selected based on the current security posture and energy states in different applications. The problem was formulated as a stochastic multi-armed bandit problem, and its optimal policy can be chosen using Gittins indices. We presented a structural results method for calculating the Gittins indices of the sensors in a large network with a variety of distributed nodes. Simulation results are presented to compare the results using the centralized scheme and the proposed distributed scheme, and the results using the structural results method and value-iteration algorithm. The system perfor-

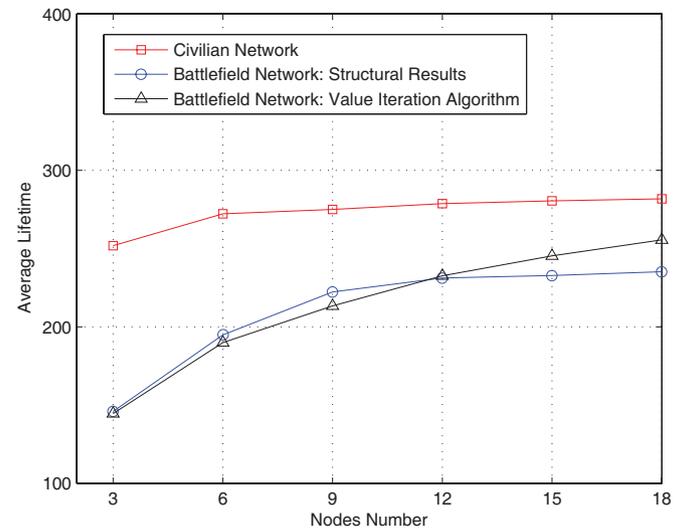


Fig. 9. Network average lifetime comparison between civilian network and battlefield network with different numbers of network nodes.

mance from the structural results method is very similar to that from the value iteration algorithm, but with much lower computational complexity. Future work is in progress to consider more nodes' states, such as mobility and wireless channels, in making the scheduling decisions in MANETs. We also plan to implement the proposed scheme in a testbed at Defence R&D Canada - Ottawa.

ACKNOWLEDGMENT

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

REFERENCES

- [1] S. Mao, S. Kompella, Y. T. Hou, H. D. Sherali, and S. F. Midkiff, "Routing for concurrent video sessions in ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 1, pp. 317–327, Jan. 2006.
- [2] T. Sim, S. Zhang, R. Janakriaman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Trans. Pattern Analysis and Machine Intell.*, vol. 29, pp. 687–700, Apr. 2007.
- [3] Q. Xiao, "A biometric authentication approach for high security ad-hoc networks," in *Proc. IEEE Info. Assurance Workshop*, June 2004.
- [4] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad-hoc networks," *IEEE Wireless Commun.*, vol. 11, pp. 48–60, Feb. 2004.
- [5] A. Azzini, S. Marrara, R. Sassi, and F. Scotti, "A fuzzy approach to multimodal biometric continuous authentication," *Fuzzy Optim. Decis. Making*, vol. 7, pp. 243–256, Sep. 2008.
- [6] J. Hu, X. Yu, D. Qiu, and H. Chen, "A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection," *IEEE Network*, vol. 23, pp. 42–47, Jan. 2009.
- [7] G. A. Jacoby and N. J. Davis, "Mobile host-based intrusion detection and attack identification," *IEEE Wireless Commun.*, vol. 14, pp. 53–60, Aug. 2007.
- [8] S. N. Chari and P. Cheng, "Bluebox: a policy-driven, host-based intrusion detection system," *ACM Trans. Inf. and Syst. Secur.*, vol. 6, pp. 173–200, May 2003.
- [9] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 806–815, Feb. 2009.
- [10] V. Krishnamurthy and B. Wahlberg, "Partially observed Markov decision process multiarmed bandits—structural results," *Math. of Oper. Res.*, vol. 34, pp. 287–302, May 2009.

[11] J. Koreman, A. C. Morris, D. Wu, and S. A. Jassim, "Multi-modal biometrics authentication on the secure phone PDA," in *Proc. Second Workshop on Multimodal User Authentication*, May 2006.

[12] A. Papanikolaou, C. Ilioudis, C. K. Georgiadis, and E. Pimenidis, "The importance of biometric sensor continuous secure monitoring," in *Proc. Third Int'l Conf. on Digital Information Management*, Nov. 2008.

[13] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Advances Signal Process.*, vol. 2008, no. 113, pp. 1–17, Jan. 2008.

[14] P. Whittle, "Multi-armed bandits and the Gittins index," *J. R. Statist. Soc. B*, vol. 42, no. 2, pp. 143–149, 1980.

[15] J.C.Gittins, *Multi-Armed Bandit Allocation Indices*. Wiley, 1989.

[16] 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.

[17] A. R. Cassandra, <http://www.cassandra.org/pomdp/code/index.shtml>, accessed 05 Oct., 2010].

[18] —, "Exact and approximate algorithms for partially observed Markov decision process," Ph.D. dissertation, Brown University, 1998.

[19] 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'04*, June 2004.

[20] Y. Liang and V. Veeravalli, "Capacity of noncoherent time-selective block Rayleigh flat-fading channel," in *Proc. IEEE Symposium of Information Theory*, June 2002.



Shengrong Bu received the B.Eng. degree in Mechanical and Automation Engineering from Huazhong University of Science and Technology, Wuhan in 2000, and the M.Eng. by Research in Electrical Engineering from University of Wollongong, Wollongong in 2005. She is pursuing the Ph.D. degree at Carleton University, Ottawa, in the Department of Systems and Computer Engineering. 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) in 2003. From 2002 to 2004, he was with Ericsson (in Lund, Sweden), where he worked on the research and development of 3G cellular networks. From 2005 to 2006, he was with a start-up in California, USA, where he worked on the 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 at Carleton University in 2007, where he is currently an Associate Professor. He received the Ontario Early Researcher Award in 2011, Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009 and best paper awards at IEEE/IFIP TrustCom 2009 and Int'l Conference on Networking 2005. His research interests include cross-layer design, security and QoS provisioning in wireless networks.

Dr. Yu is a senior member of the IEEE. He serves on the editorial boards of several journals, including *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, *ACM/Springer Wireless Networks*, *EURASIP Journal on Wireless Communications Networking*, *Ad Hoc & Sensor Wireless Networks*, *Wiley Journal on Security and Communication Networks*, and the *International Journal of Wireless Communications and Networking*. He has served on the Technical Program Committee (TPC) of numerous conferences, as the TPC Co-Chair of IEEE VTC'2012S, Globecom'11, INFOCOM-GCN'2011, INFOCOM-CWCN'2010, IEEE IWCMC'2009, VTC'2008F and WiN-ITS'2007, as the Publication Chair of ICST QShine 2010, and the Co-Chair of ICUMT-CWCN'2009.



Xiaoping P. Liu received his B.Sc. and M.Sc. degrees from Northern Jiaotong University, China in 1992 and 1995, respectively, and Ph.D. degree from the University of Alberta, Canada in 2002. He has been with the Department of Systems and Computer Engineering, Carleton University, Canada since July 2002 and he is currently a Canada Research Chair Professor. His interest includes interactive networked systems and teleoperation, haptics, micro-manipulation, robotics, intelligent systems, context-aware intelligent networks, and their applications to biomedical engineering.

Dr. Liu has published more than 150 research articles. He serves as an Associate Editor for several journals including *IEEE/ASME TRANSACTIONS ON MECHATRONICS*, *IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING*, *Intelligent Service Robotics*, *Int. J. of Robotics and Automation*, *Control and Intelligent Systems* and the *Int. J. of Advanced Media and Communication*. He received a 2007 Carleton Research Achievement Award, a 2006 Province of Ontario Early Researcher Award, a 2006 Carty Research Fellowship, the Best Conference Paper Award of the 2006 IEEE International Conference on Mechatronics and Automation, and a 2003 Province of Ontario Distinguished Researcher Award. He has served in 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 2005 IEEE International Conference on Mechatronics and Automation. Dr. Liu is a member of the Professional Engineers of Ontario (P.Eng) and a senior member of IEEE.



Helen Tang received her Ph.D. degree in the Department of System and Computer Engineering at Carleton University, Ottawa, Canada in 2005. From 1999 to 2005, she had worked in a few R&D organizations in Canada and USA including Alcatel-Lucent, Mentor Graphics and Communications Research Center Canada. In Oct. 2005, she joined Network Information Operations Section at Defence R&D Canada as a Defence Scientist. She is a member of IEEE. She has published more than 20 research papers in international journals and conferences including *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, *Journal of Security and Comm. Networks*, *IEEE ICC*, *IEEE VTC*, *IEEE Milcom*, and *IEEE Globecom*. She has served as reviewer, session chair and technical committee member for various conferences. Her research interests include ad hoc and sensor networks, wireless network security, communication protocols and performance analysis.

ences including *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, *Journal of Security and Comm. Networks*, *IEEE ICC*, *IEEE VTC*, *IEEE Milcom*, and *IEEE Globecom*. She has served as reviewer, session chair and technical committee member for various conferences. Her research interests include ad hoc and sensor networks, wireless network security, communication protocols and performance analysis.