Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks

Jie Liu, F. Richard Yu, *Senior Member, IEEE,* Chung-Horng Lung, and Helen Tang

***Abstract*—Two complementary classes of approaches exist to protect high security mobile ad hoc networks (MANETs), prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection. Most previous work studies these two classes of issues separately. In this paper, we propose a framework of combining intrusion detection and continuous authentication in MANETs. In this framework, multimodal biometrics are used for continuous authentication, and intrusion detection is modeled as sensors to detect system security state. We formulate the whole system as a partially observed Markov decision process considering both system security requirements and resource constraints. We then use dynamic programming-based hidden Markov model scheduling algorithms to derive the optimal schemes for both intrusion detection and continuous authentication. Extensive simulations show the effectiveness of the proposed scheme.**

***Index Terms*—Security, mobile ad hoc networks, authentication, intrusion detection.**

I. Introduction

IN In recent years, mobile ad hoc networks (MANETs) have become a popular research subject due to their self-configuration and self-maintenance capabilities. Wireless nodes can establish a dynamic network without the need of a fixed infrastructure. This type of network is very useful in tactical operations where there is no communication infrastructure. However, security is a major concern for providing trusted communications in a potentially hostile environment. This concern is mainly due to the peer-to-peer architecture in MANETs, system resource constraints, shared wireless medium, and highly dynamic network topology [1]. Two complementary classes of approaches exist to protect high security MANETs, prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection [2].

As the front line of defense, user authentication is crucial for integrity, confidentiality and non-repudiation [3], [4]. Authentication can be performed by using one or more of the following validation factors: something a user knows, such as a password; something a user has, such as a token or a smart card, and something a user is, such as a fingerprint or iris pattern [5]. For the password, it is simple and easy to use, but difficult to distinguish an authentic user from impostors since there is no direct connection between a user and a password. For the token, in addition to no connection between a user and a token, it is subject to being lost. Biometrics has a direct connection with the identity of the user, and has been studied in MANETs [5]. Multimodal biometrics can be used to alleviate some drawbacks of one mode of biometrics by providing multiple verifications of the same identity [6].

Most traditional authentication systems verify a user during initial login. However, for tactical MANETs in hostile environments where chances of node capture are high, it is important to verify the presence of the authentic user continuously during the lifetime of MANETs [7]. The frequency of applying authentication depends on the severity of the environment, system security requirements and resource constraints [7], [8].

The experience in security of wireline networks indicates the importance of multi-level protections because there are always some weak points in the system, no matter what is used for authentication. This is especially true for MANETs, given the low physical security of mobile devices. To solve this problem, intrusion detection systems (IDSs), serving as the second wall of protection, can effectively help identify malicious activities. An IDS continuously or periodically monitors the current subject activities, compares them with stored normal profiles and/or attack signatures, and initiates proper responses [9]. Authentication is an important type of responses initiated by an IDS. After an authentication process, only authentic users can continue using the network resources and compromised users will be excluded [10].

Although much work has been done to address continuous authentication and intrusion detection in MANETs, these two important areas have traditionally been addressed separately in the literature. In this paper, we propose to use a common framework to enable continuous authentication and intrusion detection jointly and make them share information with each other so as to obtain more efficient and cost effective mechanisms for these two processes. The motivations behind our work are based on the following observations.

- It is generally assumed that authentication decisions should be based solely on the outcome from the authentication systems (e.g., fingerprint), and intrusion detection

Manuscript received September 19, 2007; revised March 31, 2008 and July 9, 2008; accepted August 26, 2008. The associate editor coordinating the review of this paper and approving it for publication was W. Lou.

This work is supported by the Natural Science and Engineering Research Council of Canada.

J. Liu, F. R. Yu, and C.-H. Lung are with the Department of Systems and Computer Engineering, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6 (e-mail: {jieliu, chung-horng.lung}@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.2009.071036

1536-1276/09$25.00 © 2009 IEEE

should be based on a different set of information. However, the purpose of continuous authentication is to check the system security state (safe or compromised) [7], [8], which is also the main purpose of intrusion detection. Therefore, the information to solve one problem may be useful to solve another one.
- Both continuous authentication and intrusion detection may consume extensive system resources. System resource constraints are important issues in MANETs. Some examples of the constraints include limited battery power, low-power microprocessor and small memory. Considering these two processes jointly will be helpful to optimally allocate resources in MANETs.
- A common framework to enable continuous authentication and intrusion detection jointly may result in a more complex system than designing them separately. The system should be carefully designed taking into account of system security requirements and resource constraints.

To the best of our knowledge, the design of optimal combined intrusion detection and biometric-based continuous authentication considering system security requirements and resource constraints in MANETs has not been addressed in previous work. In this paper, we formulate the whole system as a partially observable Markov decision process (POMDP) [11]. The optimal policy can be acquired by solving POMDP with dynamic programming-based hidden Markov model (HMM) scheduling algorithms. Some distinct features of the proposed scheme are as follows:

- It can optimally control whether or not to perform an authentication as well as which biometrics to use to minimize the usage of system resources.
- It can optimally control whether or not to activate an IDS to minimize the usage of system resources.
- Intrusion detection and continuous authentication can share information with each other.
- System security requirement constraints and resource constraints can be guaranteed.

The rest of the paper is organized as follows. Section II describes combined intrusion detection and biometric-based continuous authentication in MANETs. Section III presents the optimal HMM scheduling algorithms, which can be used to combine intrusion detection with continuous authentication. Some simulation results are given in Section IV. Finally, we conclude this study in Section V.

II. Combined Intrusion Detection and Biometric-Based Continuous Authentication in MANETs

In this section, we first introduce biometric-based continuous authentication and intrusion detection schemes in MANETs. We then present the system model for combined intrusion detection and biometric-based continuous authentication in MANETs. Note that the authentication and intrusion detection schemes in this paper are not new. Our contribution is to combine them together and to make them share information with each other so as to obtain more efficient and cost effective mechanisms to secure MANETs.

A. Biometric-Based Continuous Authentication in MANETs

Biometrics is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioral characteristics [5]. Biometrics provides a possible solution to authentication in MANETs, because it has a direct connection with the user identity, can be continuously monitored, and needs little user interruption [5], [12]. However, biometrics is expensive to compute. The computation and comparison of biometrics usually require much more computational resources than password or token verification. This concern is more substantial in continuous authentication. Hence, the computational costs must be addressed for authentication with biometrics in MANETs.

Each biometric technology has its own strengths and weaknesses. For example, iris pattern is more accurate than voice identification, but getting a good image of the iris is difficult. Signature is a widely accepted authentication method, but it still remains a question if it could acquire the same level accuracy as the other biometric technologies. Currently, there is no best biometric modality since it depends on the environment applied. Unimodal biometrics has to face several challenges such as noise in sensed data, intra-class variations, inter-class similarities, etc [6]. Some of these problems could be resolved by adopting multimodal biometric systems. Multimodal biometric systems present more reliable authentication methods due to the combination of statistically independent biometric traits [14]. These systems can exploit the benefits of one biometric and mitigate the shortcomings of another biometric. Furthermore, randomly selecting a subset of biometric traits further ensures that the authentic user is presented.

The increasing use of multimodal biometrics has led to the investigation of different modes of system operation: serial mode, parallel mode, and hierarchical mode [6]. In serial mode of operation, one output of a biosensor will be used at one time. Therefore, multimodal biometric traits do not need to be acquired simultaneously, and the decision could be made before all biometric traits are received. The overall recognition time can be reduced, which is important for MANETs. In the parallel mode of operation, multimodal biometric traits have to be used simultaneously. The hierarchical mode of operation is suitable for the system using a large number of biometric traits. This paper will consider the serial mode of operation since it is suitable for continuous authentication in MANETs.

B. Intrusion Detection System in MANETs

Authentication is a common prevention-based approach used in MANETs to reduce intrusions. However, it cannot eliminate intrusions because there are always some weak points in the system. In MANETs, a malicious node can launch deny of service (DoS) or disrupt the routing mechanism by generating error routing messages. For these types of attacks, intrusion detection can serve as a second wall of defense and is of paramount importance in high security networks.

An IDS continuously or periodically monitors the current subject activities, compares them with stored normal profiles and/or attack signatures, and initiates proper responses [9]. Basically, IDSs can be categorized as network-based or host-based. Network-based IDSs are not suitable for MANETs

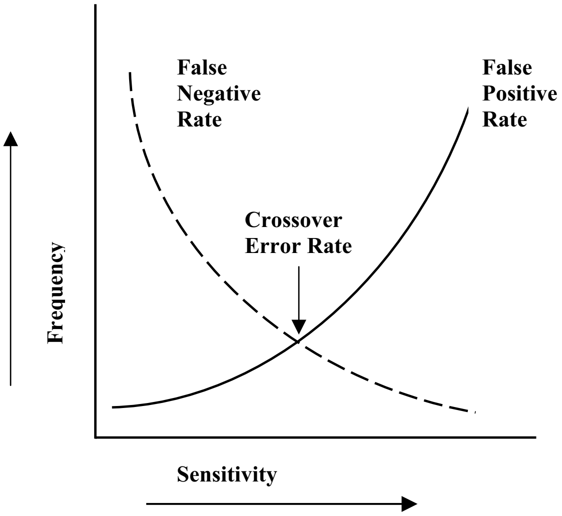


Fig. 1. Crossover error rate of IDS.

since they need to monitor or collect data that go through the network hardware interface. Host-based IDSs, which rely on data generated by users or programs located on the hosts, are good candidates for MANETs [9].

Crossover error rate (CER) is often used to provide a baseline measure for comparison of intrusion-detection systems, which is shown in Fig. 1. Here, false positive rate (FPR) is the frequency with which the IDS reports malicious activity in error, and false negative rate (FNR) is the frequency with which the IDS fails to raise an alert when malicious activity actually occurs. The selected values of FPR and FNR depend on the system security requirement. From Fig. 1, we can see that it is reasonable to model an IDS as a noisy sensor that can detect the system security state (safe or compromised). The accuracy of the noisy sensor depends on FPR and FNR of the IDS.

Intrusion detection and response systems should work collaboratively to meet the needs of MANETs. Authentication is an important type of responses initiated by an IDS. After an authentication process, only authentic users can continue using the network resources and compromised users will be excluded [10]. Note that the proposed framework is not restricted to user authentication as the only response initiated by an IDS. Other responses initiated by an IDS can also be used in this framework.

C. System Model

We assume that the MANET has a continuous authentication system, which is equipped with multiple biosensors and has the ability to collect multiple biometrics, and an IDS, which has the ability to detect intrusions. The time axis is divided into slots of equal duration that corresponds to the time interval between two operations. The length of time slot depends on the security requirements and the system environment. For instance, if the system is used in some extremely unsafe environments, the time interval can be shorter than that used in safe environments. The operations in the system include intrusion detection and authentication. In this model, if an IDS is continuously monitoring the system, the IDS is operated at all time instants. An authentication may be initiated at every time instant as well. However, the IDS and authentication may consume extensive system resources, such as battery power, which is an important issue in MANETs. Therefore, it is desirable to optimally schedule intrusion detection and authentication at each time instant taking into account system security requirements and resource constraints.

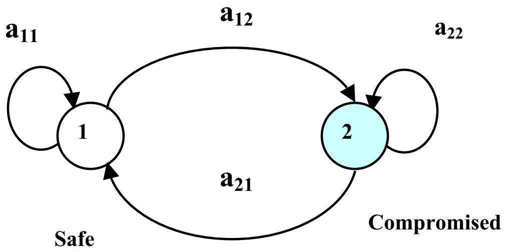


Fig. 2. State security state transition.

In modeling security systems, Markov model is a very popular approach [8], which enables rich theories developed in Markov model to be used in solving security problems. The system can be modeled as a discrete-time, 2-state (safe and compromised) first order Markov chain $\{X_k\}$, where k denotes the time instant. The state transition among these states are shown in Fig. 2. The state of the system at the time instant is X_k with state space $\{e_1, e_2\}$. Here, e_i denotes the 2-dimensional unit vector with 1 in the ith position and zeros elsewhere. The $2\times\ 2$ transition probability matrix A is defined as:

$$A = [a_{ij}]_{2\times 2}, \tag{1}$$

where $a_{ij} = P(X_k = e_j|X_{k-1} = e_i), i, j \in \{1, 2\}$.

There are several biosensors used for continuous authentication and several sensors used for intrusion detection. Altogether, there are L sensors in the system. For simplicity of the presentation, we assume that one sensor (either an authentication or an IDS) will be chosen at one time instant. Note that it is straightforward to generalize the model to picking $\bar{L}$ sensors (where $1 \leq \bar{L} \leq L$) at each time instant. In this case, both an IDS and an authentication can be run simultaneously. Let $u_k \in \{1, \ldots, L\}$ denote the sensor selected at time k, and $y_k(u_k)$ denote the observation of this sensor. The observations of the lth sensor belong to a finite set of symbols $\{O_1(l), O_2(l), \ldots, O_{M_l}(l)\}$ and $|M_l|$ denotes the number of possible observations of the lth sensor. When the system state is e_i, the lth sensor is picked at time k, the probability of observation m will be obtained from the lth sensor is denoted as:

$$\begin{aligned} b_i(u_k = l, y_k = O_m(l)) = \\ P(y_k(u_k) = O_m(u_k)|X_k = e_i, u_k = l), i = 1, 2. \end{aligned} \tag{2}$$

Define the observation matrix as:

$$\begin{aligned} B(u_k, O_m(u_k)) = \\ \text{diag}[b_1(u_k, O_m(u_k)), \ldots, b_S(u_k, O_m(u_k))], \end{aligned} \tag{3}$$

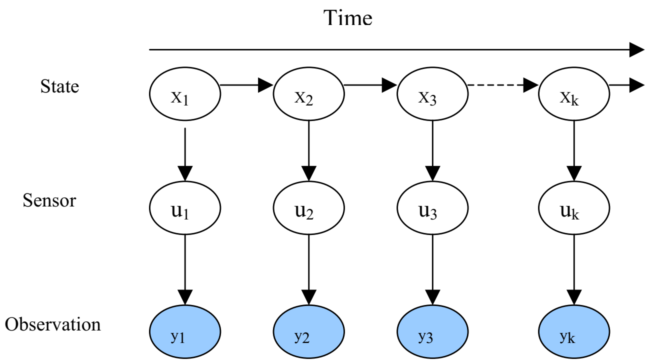


Fig. 3. Hidden Markov model.

which denotes the probabilities of the observation m acquired when the sensor u_k is picked at time k given each state of the Markov chain. The possible observations from the sensors could be "safe", "compromised", and "nothing" if no sensor is applied. The observation matrix of an IDS can be expressed as

$$B(u_k = \text{ids}) = \begin{pmatrix} 1-FPR & FPR \\ FNR & 1-FNR \end{pmatrix}. \qquad (4)$$

Note that the state of the system is not directly observed, thus the state of the system is a hidden Markov model, which is shown in Fig. 3.

There are costs associated with sensor usage: the energy consumption for computation, the information leakage if a wrong authentication/intrusion detection result is acquired, etc. To utilize the limited resources more efficiently in MANETs, an optimal scheme should be designed to optimally schedule intrusion detection and continuous authentication at each time instant to minimize the total cost in the MANET subject to system security requirement constraints and system resource constraints.

III. Solving the Combined Intrusion Detection and Continuous Authentication Problem

The partially observable Markov decision process (POMDP) [11] and relevant algorithms can be used solve the combined intrusion detection and continuous authentication problem.

A. Information State

We will refer to a probability distribution over states as an information state and the entire probability space (the set of all possible probability distributions) as the information space. For a system with two states, its information space is a one-dimension line. The distance from the right end is the first component $\pi(1)$ and the distance from the left end is the second component $\pi(2)$. For the system with 3 states, its information space is a two-dimension triangle. The value of a point in the information space can be obtained from the perpendicular distance from the sides of the triangle. An information state is a sufficient statistic for the history, which means that the optimal sensor (i.e., the optimal operation, intrusion detection or authentication) can be chosen based on the information state, denoted by π_k, where k is the time instant. Since the history information includes both intrusion detection and continuous authentication, these two processes can share information with each other so as to obtain more efficient and cost effective mechanisms for both.

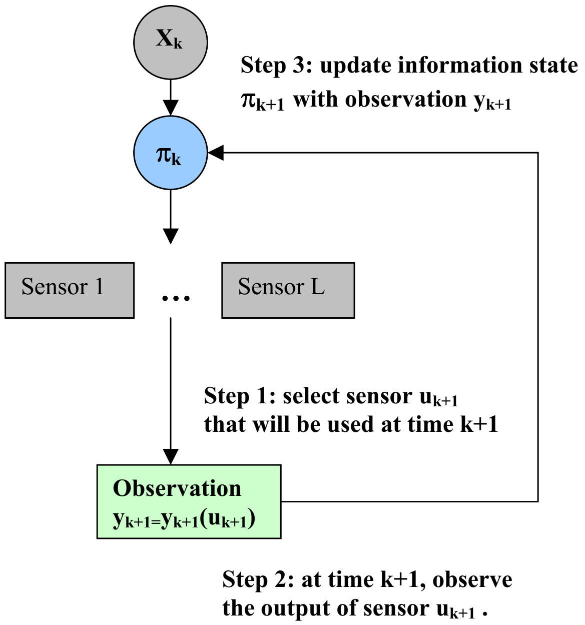

Xk
Step 3: update information state
πk+1 with observation yk+1
πk
Sensor 1
...
Sensor L
Step 1: select sensor uk+1
that will be used at time k+1
Observation
yk+1=yk+1(uk+1)
Step 2: at time k+1, observe
the output of sensor uk+1 .

Fig. 4. HMM sensor scheduling and information state update.

In our system, there are two states, and the elements of π_k is defined as:

$$\begin{aligned} \pi_k(i) &= P(X_k = e_i | Y_k), \ i = 1, 2, \\ \pi_k(1) + \pi_k(2) &= 1, \ 0 \leq \pi_k(1), \pi_k(2) \leq 1, \end{aligned} \qquad (5)$$

where $Y_k = \{u_1, u_2, \ldots, u_k, y_1, y_2, \ldots, y_k\}$, which represents the information available at time k. An important thing about information state is that it can be easily updated (see (6)) after each state transition to incorporate one additional step information into history [15]:

$$\pi_{k+1} = \frac{B(u_{k+1}, y_{k+1}(u_{k+1}))A^{'}\pi_k}{\begin{pmatrix} 1 & 1 \end{pmatrix} B(u_{k+1}, y_{k+1}(u_{k+1}))A^{'}\pi_k}. \qquad (6)$$

The initial probability vector of Markov chain is denoted as:

$$\pi_0 = [\pi_0(1), \pi_0(2)]^{'}, \text{ where } \pi_0(i) = P(X_0 = i), \ i \in \{1, 2\}.$$

By using the connection between information state and system state, a sensor can be picked based on the information state at each time instant rather than the exact system state.

B. System Architecture

With all the information above, the system procedure can be briefly summarized as three steps, which are illustrated in Fig. 4:

1) *Scheduling:* Based on the information state π_k, find the optimal sensor u_{k+1} that will be used at the next horizon.
2) *Observation:* Observe the output of the optimal sensor $y_{k+1}(u_{k+1})$ at next horizon.
3) *Update:* Update the information state π_{k+1} using the latest observation y_{k+1}.

C. Cost Definition

At time k, based on the history information $Y_k(u_k)$, sensor $u_{k+1} = l$ is selected. Then the instantaneous cost incurred at time k is:

$$\underbrace{a_k(l)\|X_k - \pi_k\|_D}_{\text{Part1}} + \underbrace{c_k(X_k, l)}_{\text{Part2}}, \tag{7}$$

where $a_k(l), l = 1, 2, \ldots, L$ are positive scalar weights and D is a quantized norm. In this paper, we select $D = l_2$. Part 1 means the square error (Euclidean distance) in the state estimation due to choosing sensor schedule $u_1, \ldots, u_k$. In biometric-based authentication, the state estimation error is closely related with the false rejection rate (FRR) and false acceptance rate (FAR). Please note that the FAR/FRR in this paper has a broader meaning than the traditional FAR/FRR. Whereas the traditional FAR/FRR of a biosensor (e.g., iris biosensor) means the false acceptance/reject rate from the biosensor, the FAR/FRR in this paper refers to the false acceptance/reject rate from the device using a biosensor for authentications. In other words, both the biosensor itself (traditional FAR/FRR) and the device (e.g, the security of the communication system) will contribute to the FAR/FRR of the biometric-based authentication system. Part 2 denotes the instantaneous cost of using sensor u_{k+1} when the system state is X_k. In MANETs, we consider this cost as battery consumption, information leaking, etc. There are many ways to make the tradeoff between immediate cost and long term cost. Here we only consider the expected future discounted cost. The cumulated cost [15] from time instant 1 to N can be expressed as:

$$J_u = E\left\{\sum_{k=0}^{N-1} a_k(u_{k+1})\|X_k - \pi_k\|_D + \right.$$
$$\left. \sum_{k=0}^{N-1} c_k(X_k, u_{k+1}) + a_N\|x_N - \pi_N\|_D \right\}. \tag{8}$$

For infinite horizon discounted cost, the cost J_u can be expressed as:

$$E\left\{\sum_{k=0}^{\infty} \beta^k [a(u_{k+1})\|X_k - \pi_k\|_D + c(X_k, u_{k+1})]\right\},$$

where the constraint $0 \leq \beta < 1$, which ensures that the expectation is bounded. What we need to do is to minimize this cost by finding the optimal sensor schedule (the optimal policy).

Considering the information state incorporated into POMDP, we define the cost as a 2-dimensional vector

$$c_k(u_{k+1}) = [c_k(e_1, u_{k+1}), c_k(e_2, u_{k+1})]'. \tag{9}$$

The cumulated cost above can be rewritten as:

$$J_u = E\left\{\sum_{k=0}^{N-1} C_k(\pi_k, u_{k+1}) + C_N(\pi_N)\right\}, \tag{10}$$

where $u_{k+1} = u_{k+1}(\pi_k)$

$$\begin{aligned} C_N(\pi_N) &= a_N g'(\pi_N)\pi_N \\ C_k(\pi_k, u_{k+1}) &= a_k(u_{k+1})g'(\pi_k)\pi_k + c_k'(u_{k+1})\pi_k \\ k &\in \{0, \ldots, N-1\}. \end{aligned} \tag{11}$$

In the above equations, $g(\pi_k)$ denotes the 2-dimensional estimation error vector:

$$g(\pi_k) = [\|e_1 - \pi_k\|_D, \|e_2 - \pi_k\|_D]'. \tag{12}$$

D. Solving the Security Problem

1) Dynamic Programming: In order to calculate (10) effectively, we will use dynamic programming to compute the optimal policy. In other words, compute this equation backward from time T to time 0. The value function (10) can be rewritten as:

$$J_N(\pi) = C_N(\pi),$$

and for $k = N-1, N-2, \ldots, 0,$

$$J_k(\pi) = \min_{u_{k+1} \in \{1,\ldots,L\}} \left[C_k(\pi, u_{k+1})\right.$$
$$+ \sum_{m=1}^{M_{u_{k+1}}} J_{k+1}\left(\frac{B(u_{k+1}, O_m(u_{k+1}))A'\pi}{(\begin{array}{cc} 1 & 1 \end{array})B(u_{k+1}, O_m(u_{k+1}))A'\pi}\right)$$
$$\left. \times (\begin{array}{cc} 1 & 1 \end{array})B(u_{k+1}, O_m(u_{k+1}))A'\pi \right], \pi \in P. \tag{13}$$

The optimal finite horizon value function of standard POMDP problem is *piecewise linear and convex* (PWLC), which was proved by Sondik [16] and Cassandra [11]. The value function of infinite horizon POMDP is not always PWLC, but it can be approximated with the value function of a large enough finite horizon POMDP. The piecewise theory is useful since the value function can be represented by a finite set of vectors such as:

$$J_k(\pi) = \min_{i \in \Gamma_k} \gamma_{i,k}'\pi \text{ for all } \pi \in P, \tag{14}$$

where Γ_k is a finite set of 2-dimensional vectors $\gamma_{i,k}'$.

2) Piecewise Linear Cost: In our case, from (11), $C_k(\pi_k, u_{k+1}) = a_k(u_{k+1})g'(\pi_k)\pi_k + c_k'(u_{k+1})\pi_k$, we can see that $g'(\pi)\pi$ is l_2 norm estimation error, which is not a linear function of π. This makes our problem different from the standard POMDP problems. Fortunately, the author of [15] has shown that this estimation error can be approximated uniformly and arbitrarily closely with piecewise linear costs:

$$g'(\pi)\pi = \min_{r \in 1,2,\ldots,R} \overline{g}_r'\pi, \tag{15}$$

where R denotes the number of 2-dimensional vectors used to approximate the estimation error. With this approximation, our sensor scheduling problem turns into a standard POMDP problem. All of the algorithms used to solve standard POMDP can be used in our case.

The quadratic cost is convex, which is shown in [15]. The upper-bound approximation using tangents [17] will be used to approximate the estimation error in our simulations.

3) Optimal Algorithm without constraints: There are several algorithms for solving finite horizon POMDP, such as Sondik's algorithm [16], incremental pruning, Cheng's linear support algorithm and the witness algorithm. Detailed explanations and corresponding programming codes of these algorithms can be found in [18]. These algorithms have the same basic framework, and the only difference is the way to compute a single dynamic programming step. The code of the incremental pruning algorithm from [18] will be modified and used in our examples. The desired solutions to POMDP are represented by a set of vectors, together with the optimal actions, and value function can be rewritten as:

$$J_k(\pi) = \min_{i\in\ \Gamma_k} \gamma^{*'}_{i,k}(u^*_{i,k})\pi \text{ for all } \pi \in P. \tag{16}$$

In this equation, each vector γ is connected with an optimal sensor. Therefore, we can solve our problem with two steps:

- ***Run off-line dynamic programming:*** Using any POMDP algorithm to compute the $\Gamma_k = \gamma^*_{k,i}$ together with the optimal sensors $u^*_{k,i}$, where $i \ \in 1, 2, \ldots, |\Gamma_k|$.
- ***Run real time scheduling:*** Find the Γ_k for specific information state $\pi(k)$ through (14). Then the optimal sensor is selected since each vector is connected with an optimal sensor.

4) Optimal Algorithm with Security Requirement Constraints: Different systems may have different security requirements. For some systems, it is desirable to guarantee FRR and FAR. In our formulation, the security requirement constraint is directly related to system security state estimation error. If the estimation error incurred by some sensors exceeds the threshold, other sensors with higher accuracy will be picked instead. Here we only consider local-in-time constraints (short term constraints) other than global constraints (long term constraints). The estimation error is specified as the expected estimation error. Our aim is to minimize the sensor usage cost subject to quadratic constraint on the expected estimation error. It is defined as:

$$J_u = \min_u E\left\{\sum_{k=0}^{N-1} c^{'}_k(u_{k+1})\pi_k\right\} \tag{17}$$

subject to:

$$\sum_{m=1}^{M_u} a_{k+1}(l)\left(1 - \frac{\pi^{'}AB^2(u,O_m(u))}{((\ 1 \quad 1\ )B(u,O_m(u))A^{\prime}\pi)^2}\right) \times(\ 1 \quad 1\ )B(u,O_m(u))A^{'}\pi) < K_l,\ l \in \zeta_c, \tag{18}$$

where ζ_c denotes the set of sensors with constraints, $\zeta_{\overline{c}}$ denotes the set of sensors without constraints, and $\zeta = \{1, \ldots, L\} = \{\zeta_c \bigcup \zeta_{\overline{c}}\}$. Therefore, the problem with security requirement constraints can be solved in the following steps:

- ***Run off-line dynamic programming with action set*** ζ : Run this program with action set ζ to get the vectors $\gamma^{\zeta}_{k,i}$ and associated optimal sensors $u^{\zeta,*}_{k,i}$.
- ***Run off-line dynamic programming with action set*** $\zeta_{\overline{c}}$: Run this program with action set $\zeta_{\overline{c}}$ to get the vectors $\gamma^{\zeta_{\overline{c}}}_{k,i}$ and associated optimal sensors $u^{\zeta_{\overline{c}},*}_{k,i}$.
- ***Run real time scheduling:*** Find the $\gamma^{\zeta}_{k,i}$ and $\gamma^{\zeta_{\overline{c}}}_{k,i}$ for specific information state $\pi(k)$ through (14). If π_k satisfies (18), then sensor $u^{\zeta,*}_{k,i}$ associated with vector $\gamma^{\zeta}_{k,i}$ will be chosen. Otherwise, sensor $u^{\zeta_{\overline{c}},*}_{k,i}$ associated with vector $\gamma^{\zeta_{\overline{c}}}_{k,i}$ will be selected instead.

5) Optimal Algorithm with System Resource Constraints: Both continuous authentication and intrusion detection may consume extensive system resources. System resource constraints are important issues in MANETs. For example, since the total energy available to a node is a scarce resource, the total number of times using a particular sensor is constraint. For simplicity of the presentation, we assume that there are only constraints on the usage of sensor 1: for N horizon problem, sensor 1 can only be used at most N_1 times. Note that it is straightforward to generalize the model to have constraints on the usage of multiple sensors.

Let $S_1 = \{f_1, \ldots, f_{N_1+1}\}$ denote the set of $N_1 + 1$ dimensional unit vectors, where f_i has 1 in the ith position. We use process z_k to denote the number of times sensor 1 is used. Let z_k be a N_1+1 state Markov chain with state space S_1. Let $z_k = f_i$ if sensor 1 has been used $i - 1$ times. The dynamics of z_k are as follows. If sensor 1 is used $(i.e., u_k = 1)$, z_k jumps to state f_{i+1}. If any of other sensors is used, z_k remains unchanged. We can express z_k as a deterministic Markov chain with dynamics given by

$$z_k = Q^{'}(u_k)z_{k-1},\quad z_0 = e_1,\ z_N = e_{N+1}, \tag{19}$$

where the transition probability matrix $Q(\cdot)$ is defined as

$$Q(u_k = 1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$\text{and } Q(u_k) = I_{(N_1+1)\times(N_1+1)} \text{ if } u_k \neq 1.$$

In order to use (13) to get the optimal scheduling policy with resource constraints, we can make the following coordinate exchange. Consider the augmented Markov chain (X_k, z_k), which has transition probability matrix $\bar{A} = A \otimes Q$, information state of (X_k, z_k) is $\bar{\pi}_k = \pi_k \otimes z_k$ and observation probability matrix $\bar{B}(u, O_m(u)) = B(u, O_m(u)) \otimes I_{N+1}$, where $\otimes$ denotes tensor (Kronecker product). Thus, the augmented information state $\bar{\pi}_k$ evolves according to the standard HMM filter with A, B replaced by $\bar{A}, \bar{B}$. Define the value function

$$\bar{J}_k = J_k(\pi, z),\ \bar{\pi} = \pi \otimes z.$$

Now we can use (13) to solve the above value function by substituting J_k with $\bar{J}_k$, π_k with $\bar{\pi}_k$, A with $\bar{A}$, and B with $\bar{B}$.

IV. Simulation Results and Discussions

In this section, we illustrate the performance of the proposed scheme by simulations. Two scenarios are considered. The first scenario involves a MANET that uses an iris sensor for user-to-system continuous authentication. In this scenario, we can model it as a two-state HMM problem with two sensors. The first one is the iris sensor. For the other one, no sensor will be used, and we estimate the system security state by using the HMM state predictor. Here we call it prediction sensor.

The second scenario involves an IDS in the MANET, which can probabilistically detect system security state, and iris-based continuous authentication. In this scenario, we can model it as a two-sate HMM problem with three sensors. The first sensor is the iris sensor. The second one is the prediction sensor, which is the same as that used in scenario 1. The IDS is treated as the third sensor.

A. Scenario 1 - Optimal Continuous Authentication

State Space: The state space is the status of the system: safe or compromised. Since the probability that the compromised system could be snatched back is usually lower compared to the probability that the safe system could be compromised, we assume that the safe system could be compromised with probability 0.3 and the compromised system could be snatched back with low probability 0.1. Thus, we obtain the following transition probability matrix of X_k:

$$A = \begin{pmatrix} 0.7 & 0.3 \\ 0.1 & 0.9 \end{pmatrix}. \tag{20}$$

Observation Symbols: When using the iris sensor, the observation symbols from the iris sensor at each time k consist of the result O_1 = safe or O_2 = compromised . Since the prediction sensor will incur nothing, we will add one more observation symbol O_3 = nothing. We define $\overline{B}_{u_k} = [\overline{B}_{ij}(u_k)] = P\{y_k(u_k) = O_j | X_k = e_i\}$. Hence, we can assign the observation matrix $\overline{B}(u_k)$ as:

$$\overline{B}(u_k = \text{iris}) = \begin{pmatrix} 0.9 & 0.1 & 0 \\ 0.1 & 0.9 & 0 \end{pmatrix}, \tag{21}$$

where we assume that FRR = FAR = 0.1.

$$\overline{B}(u_k = \text{prediction}) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{22}$$

Cost Function: There are two components in the cost function. The first component is the cost and information leakage of using the sensor.

$$c(X_k = e_i, u_{k+1} = \text{iris}) = \rho^{\text{iris}} + r^{\text{iris}},$$

$$c(X_k = e_i, u_{k+1} = \text{prediction}) = \rho^{\text{prediction}} + r^{\text{prediction}},$$

where ρ denotes the cost of using the sensor and r denotes the information leakage by using the sensor. Since using the iris sensor needs more power and memory than using the prediction sensor, we use the following values: $\rho^{\text{iris}} = 10, \rho^{\text{prediction}} = 7$, which means that the cost of using the iris sensor is higher than that using the prediction sensor. For the information leakage, since more information will be captured by the attacker if the system is in the compromised state, we use the following values for r.

$$r^{\text{iris}}(X_k = 0) = 0.5,\ r^{\text{iris}}(X_k = 1) = 2,$$

$$r^{\text{predcition}}(X_k = 0) = 1.2,\ r^{\text{prediction}}(X_k = 1) = 5.2,$$

where 0 means the safe state, and 1 means the compromised state.

The second component is the estimation error cost. For the l_2 norm estimation error,

$$g^{'}(\pi_k)\pi_k = a_k(1 - \pi_k^{'}\pi_k), \tag{23}$$

where we use $a_k = 3$ in our simulations. In order to reduce the computational complexity, we use the Lovejoy's [17] upper bound approximation. After some computations, the tangent at point π_r is the linear segment:

$$g_r^{'}(\pi_r) = (1 + \pi_r^{'}\pi_r)\begin{pmatrix} 1 & 1 \end{pmatrix}^{'} - 2\pi_r. \tag{24}$$

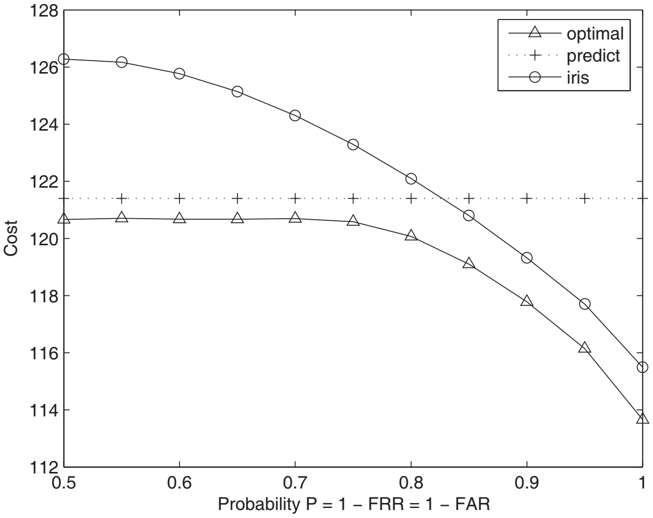


Fig. 5. Cost over infinite horizons with probability *P = 1-FAR = 1-FRR*.

With the above setups, we use the POMDP program available from the website [18] to optimally solve the HMM sensor scheduling problem. The "Incremental Pruning" algorithm is used in our simulations. All simulations are run on Redhat Linux: 3.0G CPU, 512M memory, and Kernel version is $2.4.20-31.9$. We consider the infinite horizon with discounted cost function with $\beta = 0.9$.

Results: Fig. 5 shows the cost incurred for the sensor schedule versus the probability, $P = 1 - FRR = 1 - FAR$. Here we assume that $FRR = FAR$. The costs of using the prediction sensor and using the iris sensor alone are also shown. It can be seen that when the probability P is high $(0.83 < P < 1)$, using the iris sensor has a lower cost than using the prediction sensor. The reason is that the iris sensor with high P will incur lower estimation error. Note that the FRR/FAR for the iris sensor may not be high (e.g., $0.5 < P < 0.7$) in reality. However, the security of the communication system of the device can be low (e.g., the authentication result message can be changed). This will result in a high FAR/FRR in the biometric-based authentication system. Therefore, we select a wide range for P to observe the performance of the proposed scheme. From Fig. 5, we can see that the proposed optimal scheme can have a lower cost than both selecting the prediction sensor and selecting the iris sensor alone with a wide range of P.

We then consider quadratic constraints in the estimation error, which are defined in (18). Since the observation matrix of the prediction sensor is:

$$B(u_k = \text{prediction}, y_k = 1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

(18) can be rewritten as:

$$a_{k+1}(\text{prediction})(1 - \pi^{'}AA^{'}\pi) < K_{\text{prediction}}. \tag{25}$$

In our simulations with constraints, $a_{k+1}(\text{prediction}) = 3, K_{\text{prediction}} = 1.4$, and transition matrix A is the same

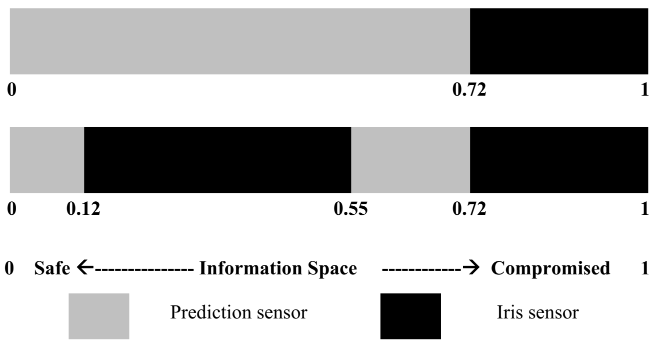

0
0.72
1
0
0.12
0.55
0.72
1
0 Safe ←--------------- Information Space ------------→ Compromised 1
Prediction sensor
Iris sensor

Fig. 6. Sensors usage over information space with and without constraints (top line – without constraints; bottom line – with constraints).

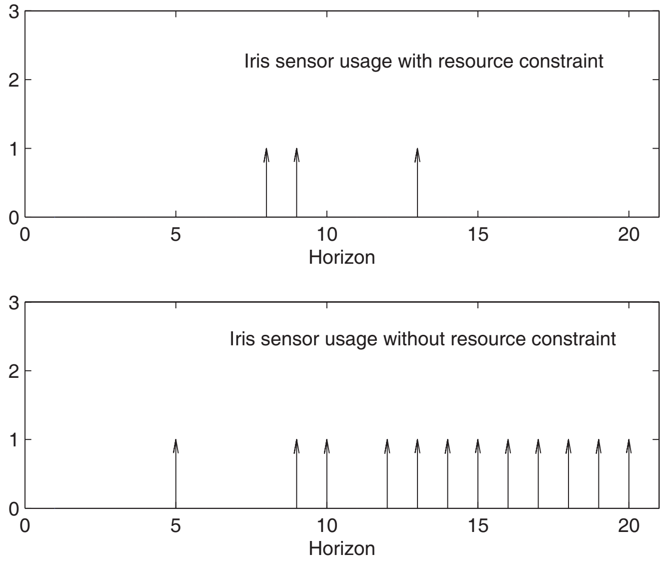


Fig. 7. Iris sensor usage when $P = 1 - FRR = 1 - FAR = 0.8$.

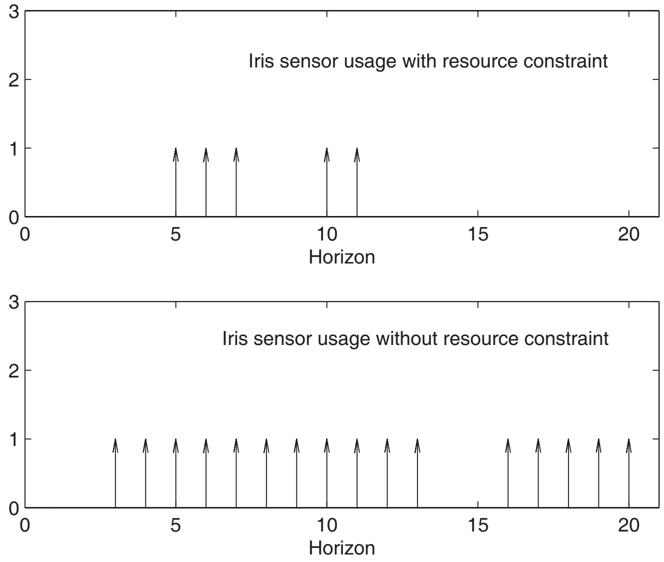


Fig. 8. Iris sensor usage when $P = 1 - FRR = 1 - FAR = 0.9$.

as (20). The observation matrix is:

$$\overline{B}(u_k = \text{iris}) = \begin{pmatrix} 0.7 & 0.3 & 0 \\ 0.3 & 0.7 & 0 \end{pmatrix}. \tag{26}$$

Fig. 6 shows the information state simplex and the optimal stationary policy for the constrained and unconstrained cases. The dark region denotes the values of π for which using the iris sensor is optimal, while the grey region denotes that using the prediction sensor is optimal. The top line shows the sensor usage without estimation error constraints, while the bottom line shows the sensor usage with estimation error constraints. Compared with the top line, one more dark region over the information space is added to the bottom line. This region means that if the prediction sensor is selected at the next time instant, the estimation error incurred by this sensor will exceed the threshold. Therefore, the more accurate iris sensor will be picked instead.

Next, we consider the resource constraints. Both authentication and intrusion detection may consume extensive system resources. Assume that the MANET is power-limited, and the iris sensor can only be used at most 5 times. According to the definition in (19), $N = 5$. There are 12 information states for this Markov process. 0 means that the system stays in the safe state and the iris sensor has never been used. $1, 2, 3, 4, 5$ mean that the system stays in the safe state and the iris sensor has been used once, twice, 3 times, 4 times, and 5 times, respectively. 6 means that the system stays in the compromised state and the iris sensor has never been used. $7, 8, 9, 10, 11$ mean that the system stays in the compromised state and the iris sensor has been used once, twice, 3 times, 4 times, and 5 times, respectively.

Fig. 7 and Fig. 8 show the simulation results of using the iris sensor with resource constraints and without resource constraints, respectively. P in the figures stands for the genuine acceptance rate and genuine rejection rate of the iris sensor. An arrow means that the iris sensor is used at that time instant. From these two figures, we can see that the iris sensor will be used for much more times if there is no resource constraints. On the other hand, if there are resource constraints in the system (the iris sensor can be used for at most 5 times), our scheme can guarantee resource constraints. The proposed scheme is desirable in reality because system resource constraints are important issues in MANETs. We also observe that the iris sensor is used for more times when $P = 0.9$ compared to the case when $P = 0.8$. The reason is that the iris sensor with higher P will incur lower estimation error, and hence lower cost. Consequently, the iris sensor can be used for more times.

B. Scenario 2 - Optimal Combined Intrusion Detection and Continuous Authentication

State space: The following transition probability matrix of X_k is used in this scenario.

$$A = \begin{pmatrix} 0.85 & 0.15 \\ 0.1 & 0.9 \end{pmatrix}. \tag{27}$$

Observation Symbols: Three observation symbols are used. The observation matrix is defined as:

$$\overline{B}(u_k = \text{iris}) = \begin{pmatrix} 0.95 & 0.05 & 0 \\ 0.05 & 0.95 & 0 \end{pmatrix}, \tag{28}$$

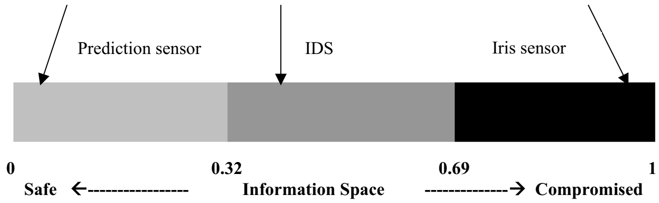


Fig. 9. Sensors usage over information space.

$$\overline{B}(u_k = \text{ids}) = \begin{pmatrix} 0.8 & 0.2 & 0 \\ 0.2 & 0.8 & 0 \end{pmatrix}, \tag{29}$$

$$\overline{B}(u_k = \text{prediction}) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \tag{30}$$

where FPR $= 0.2$, FNR $= 0.2$, and CER of the IDS is 0.2.

Cost Function: The sensor usage costs are as follows. $c(X_k = e_i, u_{k+1} = \text{iris}) = \rho^{\text{iris}} + r^{\text{iris}}$, $c(X_k = e_i, u_{k+1} = \text{prediction}) = \rho^{\text{prediction}} + r^{\text{predict}}$, $c(X_k = e_i, u_{k+1} = \text{ids}) = \rho^{\text{ids}} + r^{\text{ids}}$, where $\rho^{\text{iris}} = 11.5$, $\rho^{\text{ids}} = 7$, and $\rho^{\text{prediction}} = 4.5$. This means that the cost of using iris is higher than that using the IDS, and the cost of using the IDS is higher than that of using the prediction sensor. We set the estimation error cost as: $r^{\text{iris}}(X_k = 0) = 0.5$, $r^{\text{iris}}(X_k = 1) = 0.7$, $r^{\text{ids}}(X_k = 0) = 1.0$, $r^{\text{ids}}(X_k = 1) = 4.5$, $r^{\text{prediction}}(X_k = 0) = 1.5$, $r^{\text{prediction}}(X_k = 1) = 9$.

For the estimation error cost, we use the same method defined in (23) to approximate the quadratic estimation error.

Results: Fig. 9 shows the simulation results. The line in the figure shows the two-state information simplex. There are three regions in the figure. The left region shows the information state π for which using the prediction sensor is optimal. In the middle of the information space, it is optimal to use the IDS sensor. In the right region, using the iris sensor is optimal. Intuitively the right region indicates that the system is likely to be compromised and an authentication with the iris sensor will be needed. The left region of information space indicates that the system is in safe mode, so we do not need to authenticate this system or activate the IDS to save system resources. The middle region means that we are not certain about the status of the system. With the sensor usage costs, using the IDS to monitor the system state is the best choice. From this figure, we can see that intrusion detection and authentication can share information with each other in the proposed scheme, and it can optimally control whether or not to activate an IDS to minimize the usage of system resources.

V. Conclusions and Future Work

In this paper, we have proposed a novel framework to combine intrusion detection and continuous authentication in high security MANETs. Intrusion detection is modeled as noisy sensors that can detect the system security state (safe or compromised). Continuous authentication is performed with multimodal biometrics. We have formulated the whole system as a 2-state partially observed Markov decision process (POMDP). In this formulation, intrusion detection and continuous authentication can share history information with each other so as to obtain more efficient and cost effective mechanisms for both processes. Simulation results were presented to show the effectiveness of the proposed scheme. System security requirement constraints and resource constraints can be guaranteed.

Several new performance measures for continuous authentication are proposed in [8]. It is interesting to study these measures in the proposed scheme. In addition, further research is in progress to study the complexity of the combined system and to consider other responses initiated by an IDS in this framework.

Acknowledgment

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

References

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

[2] H. Yang, H. Luo, F. Ye, *et al.*, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[3] A. Weimerskirch and G. Thonet, "A distributed light-weight authentication model for ad-hoc networks," *Lecture Notes in Computer Science*, vol. 2288, pp. 341-354, ISBN: 3-540-43319-8, 2001.

[4] K. Ren, W. Lou, K. Kim, and Y. Fang, "A novel privacy preserving authentication and access control scheme for pervasive computing environment," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373-1384, July 2006.

[5] Q. Xiao, "A biometric authentication approach for high security ad-hoc networks," in *Proc. IEEE Info. Assurance Workshop*, West Point, NY, June 2004.

[6] A. Ross and A. K. Jain, "Multimodal biometrics: an overview," in *Proc. 12th European Signal Proc. Conf.*, Vienna, Austria, 2004.

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

[8] T. Sim, S. Zhang, R. Janakriaman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[9] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," *Mobile Net. and App.*, vol. 9, no. 5, pp. 45-56, Sept. 2003.

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

[11] A. R. Cassandra, "Exact and approximate algorithms for partially observed Markov decision process," Ph.D. dissertation, Brown Univ., 1998.

[12] J. Koreman, A. C. Morris, D. Wu, S. A. Jassim, *et al.*, "Multi-modal biometrics authentication on the Securephone PDA," in *Proc. 2nd Workshop on Multimodal User Auth.*, Toulouse, France, May 2006.

[13] A. J. Klosterman and G. R. Ganger, "Secure continuous biometric-enhanced authentication," CMU SCS Technical Report CMU-CS-00-134, May 2000.

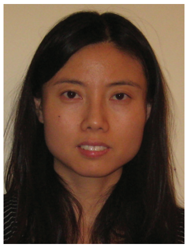
[14] A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Lett.,* vol. 24, pp. 2115-2225, Sept. 2003.

[15] V. Krishnamurthy, "Algorithms for optimal scheduling and management of hidden Markov model sensors," *IEEE Trans. Signal Processing*, vol. 50, no. 6, pp. 1382-1397, June 2002.

[16] R. D. Smallwood and E. J. Sondik, "Optimal control of partially obervable Markov processes over a finite horizon," *Oper. Res.*, vol. 21, no. 5, pp. 1071-1088, 1973.

[17] W. S. Lovejoy, "Computationally feasible bounds for partially observed Markov decision processes," *Oper. Res.*, vol. 39, no. 1, pp. 162-175, 1991.

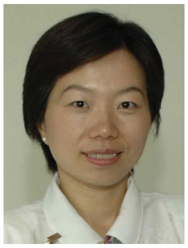
[18] A. R. Cassandra, "Tony's POMDP Web page." [Online]. Available: http://www.cs.brown.edu/research/ai/pomdp/index.html.



Jie Liu received her B.Eng. degree from Beijing University of Posts and Telecommunications, in 1994, and the M.Eng degree from Carleton University in 2007. From 2001 to 2004, she had worked on research and development in the areas of CDMA2000 and WCDMA in Ericsson China. She joined Ericsson Canada in 2007 and is now working on IP Multimedia System.

F. Richard Yu 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, Canada, in 2006, where he is currently an Assistant Professor. His research interests include cross-layer design, QoS provisioning and security in wireless networks. He has served on the Technical Program Committee (TPC) of numerous conferences and as the TPC Co-Chair of IEEE IWCMC'2009, VTC'2008F Track 4, WiN-ITS'2007. He is a senior member of the IEEE.

Chung-Horng Lung received his B.Eng. degree in Computer Science and Engineering from Chung-Yuan University, Taiwan, in 1983, and the M.S. and Ph.D. degrees in Computer Science and Engineering from Arizona State University in 1988 and 1994 respectively. In September 2001, he joined the Department of Systems and Computer Engineering, Carleton University, Ottawa, Canada, where he is now an associate professor. He was with Nortel Networks from 1995 to 2001. At Nortel, he worked in the Software Engineering Analysis Lab (SEAL) as a senior software engineer and architect, and Optical Packet Interworking (OPi) as a senior software designer for advanced traffic engineering. He worked in the Electronics Research and Service Organization (ERSO), Taiwan, in 1985. His research interests include: Communication Networks, Wireless Ad Hoc and Sensor Networks, Distributed & Parallel Computing, Software Engineering, and Network-Based Control Systems.



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 COMMUNICATIONS 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.