A Novel Approach to Combine Misuse Detection and Anomaly Detection Using POMDP in Mobile Ad-Hoc Networks

Mohsen Imani, Mohammad Ebrahim Rajabi, Mahdi Taheri, and Majid Naderi

***Abstract*—Security becomes out of the main concerns in mobile ad hoc networks. Intrusion detection systems are reactive systems that act as a second wall to protect the network. Misuse detection is a technique which is used commonly by intrusion detection systems to match the attack-signature pattern in mobile ad hoc networks. Anomaly detection is another technique that is able to detect novel attacks. Both of the misuse detection and the anomaly detection techniques monitor system activities. The weak point of misuse detection is the disability in detection of unknown attacks. Anomaly detection is able to detect unknown attacks but false positive rate in anomaly detection responses is so high. Therefore in this paper we take advantages of combination schemes to overcome the shortco-ming of each technique. We propose a novel approach to combine the misuse detection with the anomaly detection optimally to save cost associated with resource constraints and security requirements. We perform the whole system as a partially observed Markov decision process considering both system security and resource constraints. We then use dynamic programming Hidden Markov Model (HMM) to share information history and scheduling. Simulation shows the efficiency of proposed scheme.**

***Index Terms*—Component, mobile ad hoc networks, intrusion detection, misuse detection, anomaly detection.**

I. Introduction

In recent years wireless mobile ad hoc networks (MANETs) have received significant attention due to their features like self configuration and self maintenance. Mobile Nodes can communicate through wireless links and establish dynamic networks without the need of fixed infrastructure. The network topology is constantly chang-ing as joining or moving nods out. All of the network operation is carried out by the individual node themselves. With development of MANET applications, security becomes out of the main concerns, this concern is mainly due to open network architecture, shared wireless medi-um, resource constraints and highly dynamic topology [1]. The absence of centralized management and limited phy-sical protection increases vulnerability and attacks in these networks.

There are two major security approaches in MANETs: protection approaches such as authentication that attempts to prevent an attacker from launching attack in first place. The second one is reactive approaches such as intrusion detection system (IDS) that seeks to detect security treats and attacks [2].

With wire line network study, there is some weak points in prevention systems no matter what kinds are used. Hence the second line of defense is essential to increase the system security level. Intrusion detection system (IDS) works as dogwatch that is capable to monitor network activities continuously or periodically compares them with stored data and initiate proper response [2]. There are two kind of attacks: known attacks and unknown attacks, the known attacks are attacks which they have taken place before and the signatures of them is stored in the system database, then an IDS can match the attack signature with database using misuse detection technique and detect the attack. Otherwise there are no previous stored signatures for unknown attacks, because these attacks takes place for first time and misuse detection technique is not capable to detect this kind of attacks. The anomaly detection technique involves looking for behavior which is outside the normal expected behavior. This is usually done by utilizing statistical techniques that compare the observed behavior against the statistics of the expected normal behavior. Both of the misuse detection and the anomaly detection technique have their own advantages and disadvantages. In this paper we propose a novel approach to combine the misuse detection with the anomaly detection technique to monitor the network and host activities collaboratively and check the attack type (known or unknown). We use partially observed Markov decision process (POMDP) to solve combination problem. The optimal policy can be acquired by solving POMDP with dynamic programming based hidden Markov model (HMM) scheduling algorithms.

The rest of the paper is organized as follows. Section II describes related works done in intrusion detection and combination schemes. Section III presents an overview of intrusion detection systems. In Section IV we propose our scheme. A simulation result is shown in Section V. Finally, we conclude this study in Section VI.

II. Related Works

Hybrid detection techniques were studied in traditional networks. ADAM (Audit Data Analysis and Mining) [3] is the one of the most widely known project in this field. It is an on-line network-based IDS. ADAM uses association rules algorithm in detection. The Next Generation Intrus-ion Detection Expert System (NIDES) which developed by SRI [4] is a hybrid intrusion detection system. NIDE performs

Manuscript received September 11, 2014; revised November 18, 2014.

The authors are with Cryptography and Secure Systems Lab, Iran university of Science and Technology, Tehran, Iran (e-mail: moh.imani@ieee.org, merajabi@elec.iust.ac.ir, mahdi_taheri@elec.iust.ac.ir, m_naderi@iust.ac.ir).

DOI: 10.7763/IJIEE.2015.V5.538

real-time monitoring of user activity on multiple target systems connected on a network. It consists of a misuse detection component as well as an anomaly detect-ion component. In this paper, we try to implement a novel combination scheme in mobile ad hoc networks. The advantage of our scheme is to optimally combine misuse detection with anomaly detection to reach the high level of accuracy in intrusion detection systems in deal with cost constraints.

III. Intrusion Detection Systems

There are some weak points no matter what kind of prevention systems is used. They especially grow up in MANETs with low physical security. IDS acts as a background that monitors network and host activities, analyses their behavior and compares them with stored normal profile or attack signatures, then it can initiate proper response.

There are three types of function at intrusion detection systems: 1) anomaly detection which creates a profile of normal system's activity derivation from base line trended as possible intrusions. 2) Misuse detection, which IDS utilize an expert system to identify intrusions based on predetermined knowledge, legal or illegal behavior can be defined and observed data is compared according signature base. 3) Specification based detection: at first it defines a set of constraints to describe the current operation of a program or protocol and monitors the execution of program with respect to defined constrains. This technique may provide capability to detect previous-ly unknown attacks [5]. Implementing this technique is not desirable in MANETs due to cost associated in resource consumption and complex processes.

IV. Proposed Scheme

There are some restrictions in MANETs: resource constraints such as low battery power, small memory, and weak processor. Due to these restrictions the motivations behind our work are based on the following observations:

- Both of the misuse detection and the anomaly detection may consume extensive system resources. Some kinds of the constraints include limited battery power, weak microprocessor and small memory. Considering the misuse and the anomaly detection jointly, will be helpful to optimally allocate resources in MANETs.
- A common framework to enable the misuse detect-ion and the anomaly detection jointly may result in a more complex system than designing each other separately. The system should be carefully designed taking into account of system security requirements and resource constraints.

In this paper we use the misuse detection as a technique with high ability of known attack detection and the anomaly detection technique with high ability of unknown attack detection. We formulate whole system as partially observed Markov decision process (POMDP). We solve POMDP with dynamic programming based Hidden Markov Model (HMM) for scheduling the techniques and considering the cost optimally.

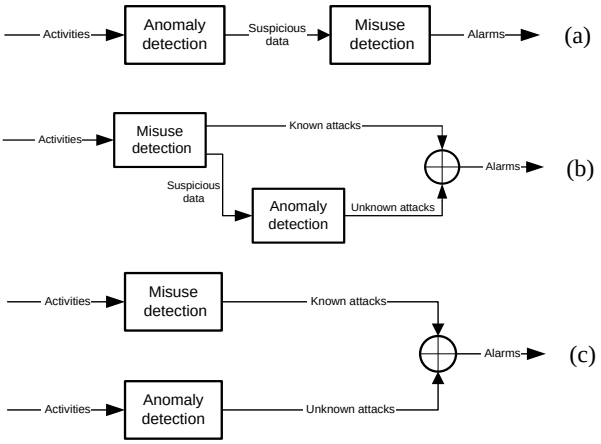

Fig. 1. Combination methods. (a) Sequential approach: anomaly followed by misuse. (b) Sequential approach: misuse followed by anomaly (hybrid detection). (c) Parallel approach.

A. Combination

In order to reach the accuracy of a misuse detection system and have the ability to deal with new attacks, we proposed the combination scheme. There are three ways to combine the misuse and the anomaly detection:

1) Sequential mode.
2) Parallel methods.
3) Serial approach.

These three ways are shown in Fig. 1 and Fig. 2. Sequential mode is depicted in Fig. 1a and Fig. 1b, for example in anomaly detection followed by misuse detection at first, observed activities is fed into the anomaly detection component. The component produces suspicious items that deviate from the built normal profile. Then, the misuse detection component identifies intrusions from the suspicious items. The items that match patterns of attacks are determined as known attacks. The items that match patterns of false alarms are determined as normal activities. The others are determined as unknown attacks. In this approach, the anomaly detection component should have high detection rate, since some intrusions cannot be detected by the follow-up misuse detection component. The misuse detection component should be able to identify false alarms. The false positive rate can be reduced by excluding the false alarms from the suspicious items. Another connection in sequential mode is depicted in Fig. 1b; in this approach, observed activities are fed into the misuse detection component. The component applies the algorithm to detect known attacks by matching the patterns of attacks. Other items (uncertain items) that do not match any pattern are fed to the anomaly detection component to detect unknown intrusions using the outlier detection.

Fig. 1c shows the framework of the parallel method. Observed activities are fed to the misuse detection and the anomaly detection component in parallel. The two sets of suspicious items are produced by them. The correlation component analyzes these two sets to detect intrusions.

In serial mode of operation, one output of a system will be used at one time. Therefore, the overall recognition time can be reduced which is important in MANETs. We

propose a serial approach as exhibited in Fig. 2. According to the attack type (known or unknown) at each time instant only one system can be selected. The misuse detection is used when the probability of known attack is high. Whenever the probability of unknown attack increases and reaches the threshold, the switch changes to the anomaly detection and in this time unknown attack can be detected with high detection rate using the anomaly part. As shown in Fig. 2, the output of unknown rate of the misuse and the anomaly detection is fed to a comparator. The output of the comparator is 0/1, if known attack rate is high the output is 0 and switch changes to the misuse detection and whenever unknown attack detection rate increases it is 1 and switch will change to the anomaly detection, therefore dynamic scheduling can control using comparator. Both systems can share history information with each other and also as a novel attack is detected in the anomaly detection part the system can update misuse detection database for future detections. This approach allows dynamically updating database to reach the high accuracy of detection according to constraints in MANETs.

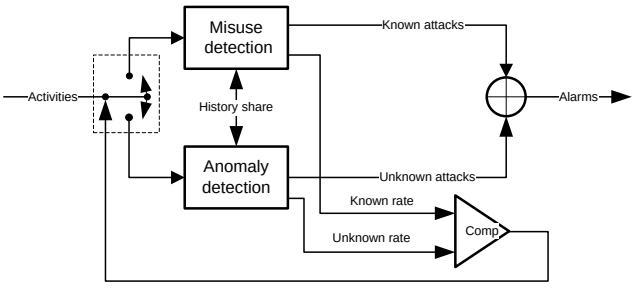

Fig. 2. Proposed scheme, serial mode.

B. Problem Formulation

Markov model is very popular approach in modeling security systems. There are four components in modeling POMDP: a set of states, a set of actions, the effect of the actions and the immediate value (cost/ reward) of the actions also we need the accumulate cost function to calculate cast. We describe our scheme as follows.

States: we can describe our model as two states (known/unknown). The state of the system at the time instant is X_k with state space of $\{e_1, e_2\}$, Here, e_i denotes the 2-dimensional unit vector with 1 in the *i*-th position and zeros elsewhere.

Actions: The actions are the possible options that we can make; the actions in our model are the misuse detection and the anomaly detection. Each action has an observation that can be defined with matrix as below:

$$B\big(u_k, O_k(u_k)\big) = diag[b_1\big(u_k, O_k(u_k)\big), \dots, b_s\big(u_k, O_k(u_k)\big) \quad (1)$$

where $u_k \in \{1, \dots L\}$ denotes the action selected at time k, in our model $= 2$. $O_m(u_k)$ Denots the n-th observation of action u_k and b_i defined as follow.

$$b_i\big(u_k = L, O_m(L)\big) = P(O_m(u_k)|X_k = e_i, a_k = l), i = 1,2. \quad (2)$$

Transitions: The transition specifies how each of the actions changes the state. We can describe transition matrix *A* as below:

$$A = [a_{i\,j}]_{2\times 2}, \quad where\ a_{i\,j} = P(X_k = e_j | X_{k-1} = e_i) \quad i, j \in \{1, \dots, s\}. \quad (3)$$

We have two states then in equation (3) *s* is equal to *2*.

Cost: Each action has an appropriate value which defines with award or cost in genuine POMDP model, we deal with cost term. Immediate cost acquired at time of k is:

$$a_k(l)||X_k - \pi_k||_D + c_k(X_k, l) \quad (4)$$

In order to describe equation (4) we can slice it into two parts:

First part: $a_k(l)||X_k - \pi_k||_D$, denotes state estimation error, D is a quantized norm that we choose $D = l_2$ (Euclidian distance). $a_k(l), l = 1,2, \dots, L$ are positive scalar weights, L is the number of actions, and π_k denotes the information state that can be easily updated into history [6].

$$\pi_{k+1} = \frac{B\big(u_{k+1}, y_{k+1}(u_{k+1})\big)A'\pi_k}{(1\ 1)B\big(u_{k+1}, y_{k+1}(u_{k+1})\big)A\pi_k} \quad (5)$$

In equation (5) B is observation matrix which $u_k \in \{1, \dots, L\}$ denotes the technique selected at time *k*, and $y_k(u_k)$ denotes the observation of this technique (known/ unknown), and *A* is the transition matrix as described before.

Second part: $c_k(X_k, l)$ denotes the immediate cost of utilizing each action. We consider cost of battery consumption and the information leakage.

There are many ways to make the tradeoff between the immediate cost and the long term cost. Not that we only consider the expected future discounted cost. The cumulated cost [7] from time instant *1* to *N* can be expressed as:

$$J_u = E\left\{\sum_{k=0}^{N-1} a_k(u_{k+1})\big||X_k - \pi_k|\big|_D + \sum_{k=0}^{N-1} c_k(X_k, u_{k+1}) + a_N\big||x_N - \pi_N|\big|_D\right\} \quad (6)$$

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

$$J_u = E\left\{\sum_{k=0}^{\infty} \beta^k\big[a_k(u_{k+1})\big||X_k - \pi_k|\big| + c_k(X_k, u_{k+1})_D\big]\right\} \quad (7)$$

where the constraint is $0 \le \beta < 1$, 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).

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

$$c_k(u_{k+1}) = [c_k(e_1, u_{k+1}), c_k(e_2, u_{k+1})]' \quad (8)$$

The cumulated cost above can be written as:

$$J_u = E\left\{\sum_{k=0}^{N-1} C_k(\pi_k, u_{k+1}) + C_N(\pi_N)\right\} \quad (9)$$

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

$$\begin{aligned} C_N(\pi_k) &= a_N g'(\pi_N)\pi_N \\ C_k(\pi_k, u_{k+1}) &= a_k(u_{k+1})g'(\pi_k)\pi_k \\ &\quad + c'_k(u_{k+1})\pi_k \\ k &\in \{0, \dots, N-1\} \end{aligned} \quad (10)$$

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

$$g(\pi_k) = [\|e_1 - \pi_k\|_D, \|e_2 - \pi_k\|_D]' \quad (11)$$

C. Solving Optimal Algorithm with Cost Constraints

There are several algorithms for solving finite horizon POMDP [8], such as Syndic's algorithm, Incremental pruning, Cheng's linear support algorithm, and the witness algorithm.

Incremental pruning is a simple, fast and exact method for solve POMDP problem [9]. The code of incremental pruning algorithm from [8] will be modified and used in our examples. The desired solutions to POMDP are represented by a set of vectors, along with the optimal actions, and value function can be rewritten as:

$$J_k(\pi) = \min_{i \in \Gamma_k} \gamma'_{i,k}(u_{i,k})\pi \ \ and\ \pi \in P. \quad (12)$$

In equation (12), Γ_k is a finite set of 2-dimensional vectors and each vector γ is connected with an optimal sensor. Therefore, we can solve our problem with two steps:

Step1: Using incremental pruning algorithm to compute the $\Gamma_k = \gamma_{i,k}$ along with the optimal actions $u_{i,k}$ where $i \in 1, 2, \dots, |\Gamma_k|$.

Step2: Find the Γ_k for specific information state $\pi(k)$ through equation (5). Then the optimal action is selected since each vector is connected with an optimal action.

V. Simulation Results

In this section, we demonstrate our scheme with simulation. We utilize incremental pruning algorithm available in website [8]. We run pomdp-solve program for simulation. The POMDP file parameter set as follow:
Discount factor =0.95.

States: The state in our scheme is: known and unknown. We assume that the known attacks could be change to unknown with probability of 0.1 and the unknown attacks could be snatched back with high probability 0.35. Thus, we obtain the following transition probability matrix:

$$A = \begin{bmatrix} 0.9 & 0.1 \\ 0.35 & 0.65 \end{bmatrix} \quad (13)$$

Actions: There are two actions in our simulation: misuse and anomaly. The observation from each system at time k consist of the result O_1 = known or O_2 = unknown. With assumption of FPR (false positive ratio) = FNR (false negative ratio) = 0.1 for misuse detection we can construct observation matrix as below.

$$B(u_k = misuse) = \begin{bmatrix} 0.9 & 0.1 \\ 0.1 & 0.9 \end{bmatrix} \quad (14)$$

For anomaly detection we assume that FPR=FNR=0.25 then the observation matrix is

$$B(u_k = anomaly) = \begin{bmatrix} 0.75 & 0.25 \\ 0.25 & 0.75 \end{bmatrix} \quad (15)$$

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

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

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

where ρ denotes the cost of using the technique and r denotes the information leakage by using the technique. Since utilizing the anomaly needs more power than the misuse and otherwise it has low information leakage rather than misuse when attacks are unknown, we set cost as follow:

$$\rho^{misuse} = 6\,,\ \rho^{anomaly} = 4,$$

$$r^{misuse}(X_k = 0) = 1,\ r^{misuse}(X_k = 1) = 8,$$

$$r^{anomaly}(X_k = 0) = 5.5,\ r^{anomaly}(X_k = 1) = 6.5,$$

where 0 is the known attack state and 1 is the unknown attack state.

We then consider nonlinear cost for estimation error which is defined in equation (11) we consider the l_2 cost $\alpha_k(1 - \pi'_k\pi_k)$. We choose $\alpha_k = 3$.

With the above setting, we use the program pomdp-solve v5.3 available from the website [8] to optimally solve the HMM sensor scheduling problem. The "Incremental Pruning" algorithm is used in our simulations. All simulations are run on fedora 10 Linux: 2.4GHz CPU, 512M memory, and Kernel version is 2.6.27.5−117. We consider the infinite horizon with discounted cost function 0.95.

Results: Fig. 3 shows the cost incurred for the sensor schedule versus the probability of unknown attack. The cost of using the misuse technique and using the anomaly technique alone is also plotted. It can be seen that when the probability p is high $(0.24 < p < 1)$, using the anomaly technique has a lower cost than using the misuse technique. The reason is that the anomaly technique with high p wills occurs in lower estimation error. From Fig. 3, we can see that the proposed optimal scheme can have a lower cost than both selecting the misuse technique and selecting the anomaly technique alone with a wide range of p.

Fig. 4 shows two regions in scheduling policy. The left region shows the information state π for which using the misuse detection technique is optimal. In the right hand side of the information space, it is optimal to use the anomaly

detection technique. Instinctively the right region indicates that the system is likely to be unknown attack and anomaly detection will be needed.

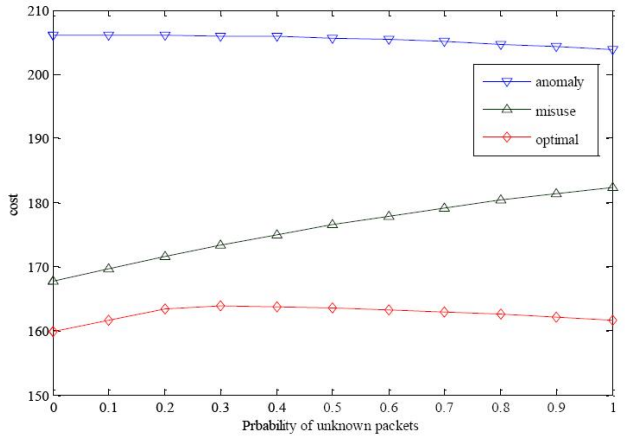

Fig. 3. comparison of cost between individual technique usage and optimal technique selection.

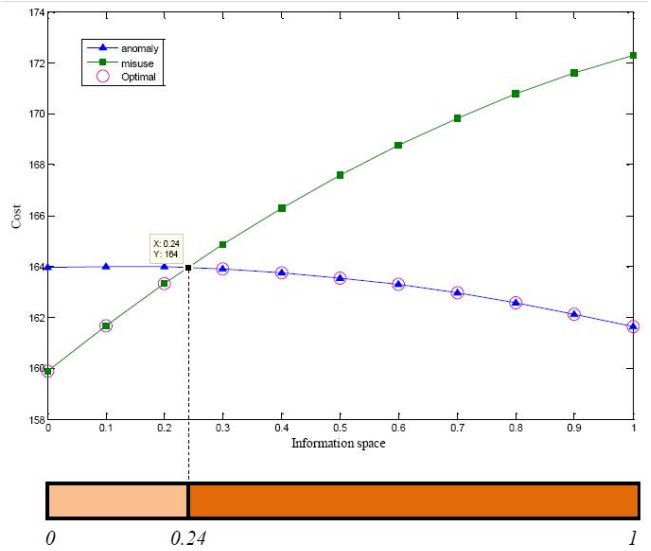

Fig. 4. Technique usage over information space with cost constraints.

The left region of information space indicates that the system is in known attack mode, so we do not need to use anomaly detection as discussed before. Simulation results show the effectiveness of proposed scheme, so it can optimally control whether or not to activate misuse detection technique or anomaly detection technique to minimize the usage of system resources.

VI. Conclusion

In this paper, we proposed a novel approach to optimally combine the misuse detection technique with the anomaly detection technique. The misuse detection has high accuracy in known attack detection but it is unable to detect novel attack. On the other hand anomaly detection technique has high false positive rate but is able to detect novel attack. In the proposed framework we combined these techniques to mitigate the shortcomings of each other along with cost constraints.

We formulated the whole system as a 2-state partially observed Markov decision process (POMDP). In this formulation the misuse detection and the anomaly detection can share history information with each other so as obtain more efficient and cost effective mechanisms for both processes. The simulation result approves the proposed scheme.

References

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2] 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.

[3] D. Barbarra, J. Couto, S. Jajodia, L. Popyack, and N. Wu, "ADAM: Detecting intrusions by data mining," *IEEE Workshop on Info. Assurance and Sec.*, pp. 11-16, June 2001.

[4] D. Anderson, T. Frivold, and A. Valdes, "Next-generation intrusion detection expert system (NIDES) - A summary," Technical Report SRICSL -pp. 95-07, SRI, May 1995.

[5] F. Sabahi and A. Movaghar, "Intrusion detection: A survey," in *Proc. IEEE the Third Conf. on Sys. and Net. Commun.*, pp. 23-26, Aug. 2008.

[6] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *J. IEEE*, vol. 77, pp. 257–285, 1989.

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

[8] Pomdp-solve- available. [Online]. Available: http://www.pomdp.org/

[9] A. R. Cassandra, M. L. Littman, and N. L. Zhang, "Incremental pruning: A simple fast exact method for partially observed Markov decision processes," presented at 13th Annu. Conf. Uncertainty Artif. Intell., 1997.

Mohsen Imani received his BS degree in electrical engineering in 2004 from Shahrood University of Technology and his master degree in the same field from Iran University of Science and Technology (IUST) in 2011. He was a member of Secure System Lab at IUST from 2008 to 2011. His research interests are network security and communication networks. Currently he is doing his PhD in computer science at the University of Texas at Arlington.