A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks[*]

Yu Liu
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030, USA
Yu.Liu@stevens.edu

Cristina Comaniciu
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030, USA
Cristina.Comaniciu@stevens.edu

Hong Man
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030, USA
Hong.Man@stevens.edu

ABSTRACT

In wireless ad hoc networks, although defense strategies such as intrusion detection systems (IDSs) can be deployed at each mobile node, significant constraints are imposed in terms of the energy expenditure of such systems. In this paper, we propose a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation. We study the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios. The dynamic Bayesian game is a more realistic model, since it allows the defender to consistently update his belief on his opponent's maliciousness as the game evolves. A new Bayesian hybrid detection approach is suggested for the defender, in which a lightweight monitoring system is used to estimate his opponent's actions, and a heavyweight monitoring system acts as a last resort of defense. We show that the dynamic game produces energy-efficient monitoring strategies for the defender, while improving the overall hybrid detection power.

Categories and Subject Descriptors

H.5 [**Information Interfaces and Presentation**]: Miscellaneous

General Terms

Security, Design

Keywords

ad hoc network, noncooperative game, Bayesian game, attacker/defender game

1. INTRODUCTION

Ad hoc networks are infrastructure-free, self-organized systems, for which the network operation is based on cooperation of nodes within the neighborhood. In an open environment (i.e. no pre-existing trusted authority), each node agrees to perform network functions such as forwarding and routing. Besides selfishness, ad hoc network misbehavior may be inflicted by malicious nodes, each of which intentionally aims at harming the network operation. A malicious node can mount attacks against different network layers to either compromise individual node(s) or degrade the performance of the overall network. Moreover, existing protocols and techniques for ad hoc networks do not limit end users to use them in a WLAN environment. Hence, if a malicious node can form an ad hoc network with a legitimate WLAN station, it can compromise this station, and then use it as a "backdoor" into the WLAN to stage attacks. Therefore, malicious behavior in ad hoc networks can reach to WLANs and wired networks.

IDSs are important means to detect malicious node behavior. In ad hoc networks, most IDSs are proposed to individual nodes (e.g. [1, 2, 3, 4]) due to the lack of centralized management. To better defend a network, every defending node is suggested to be equipped with an IDS, and each IDS is assumed to be always-on. That is to say, each defending node has to be in *promiscuous* mode. From a system usage perspective, always-on is not an efficient option because mobile nodes are often resource-constrained. To improve defender's monitoring efficiency, a game-theoretic approach is suggested to model the interactions between attacking node (attacker) and defending node (defender).

We formulate the attacker/defender game model in both static and dynamic Bayesian game contexts, and investigate the equilibrium strategies of the two players. The motivation behind our Bayesian game formulation is that generally an attacker/defender game is an incomplete information game [5, p209] where the defender is uncertain about the type of his opponent (regular or malicious). A Bayesian game formulation provides a framework for the defender to select his strategies based on his belief on the type of his opponent.

The difference between a static and a dynamic Bayesian game is that the former does not take into account the game evolution, and the defender has fixed prior beliefs about the types of his opponent. In contrast, the latter is a more re-

[*] This work was supported in part by the ONR grant number N00014-06-1-0063.

Valuetools '06, October 11-13, 2006, Pisa, Italy.
Copyright 2006 ACM 1-59593-507-X ...$5.00.

alistic game model, because the defender can dynamically update his beliefs based on new observations of the opponent's actions and the game history, and then can adjust his monitoring strategy accordingly.

In the dynamic game model, a new Bayesian hybrid detection approach is suggested for the defender, with one being used as a lightweight monitoring system to estimate his opponent's action in each stage game, and the other being used as a heavyweight monitoring system, which functions as a last resort of defense. The heavyweight monitoring system is assumed to have more detection power than the lightweight monitoring system, e.g., can resolve attack sources or has higher detection rate. We show that the dynamic game produces energy-efficient monitoring strategies for the defender, while improving the overall hybrid detection power.

The rest of the paper is organized as follows. Section 2 introduces the static Bayesian game model, and Bayesian Nash equilibrium solutions are investigated. Section 3 describes the dynamic Bayesian game model, and perfect Bayesian equilibrium solutions are studied. Section 4 considers multiplayer scenarios for both game models. Section 5 presents numerical examples for the proposed games. Section 6 discusses related work. Finally, Section 7 concludes the paper.

2. STATIC BAYESIAN GAME

2.1 Game Model

Consider a flat ad hoc network with a fixed number of N nodes in the network. It is assumed that any defending node is equipped with an IDS. Depending on the capability of the IDS, the defending node can detect an attacking node in the neighborhood or any node in the network.

We consider a two-player static Bayesian game. One player is a *potential* attacking node, denoted by i. The other player is a defending node, denoted by j. Player i has private information about his type, which is either regular, denoted by $\theta_i = 0$, or malicious, denoted by $\theta_i = 1$. In other words, the maliciousness of player i is unknown to defender j. Defender j is of regular type denoted by $\theta_j = 0$. The type of defender j is common knowledge to the two players.

The malicious type of player i has two pure strategies: *Attack* and *Not attack*. The regular type of player i has one pure strategy: *Not attack*. Defender j has two pure strategies: *Monitor* and *Not monitor*. The two players choose their strategies simultaneously at the beginning of the game, assuming common knowledge about the game (costs and beliefs).

Assume defender j's security value is worth of w, where $w > 0$. In practice, w could be the (monetary) value of protected assets. In other words, $-w$ represents a loss of security whose value is equivalent to a degree of damage such as *loss of reputation*, *loss of data integrity*, *cost of damage control*, etc. Therefore w is subject to different security policies. We also assume that there is an equal gain/loss w for both the defender and the attacker. This is reasonable when dealing with malicious nodes (as opposed to selfish nodes).

Table 1 illustrates the payoff matrix of the game in strategic form. In the matrix, α represents the detection rate (i.e. true positive rate) of the IDS, β represents the false alarm rate (i.e. false positive rate) of the IDS, and α, $\beta \in [0, 1]$. w is defender j's security value. Costs of attacking and monitoring are denoted by c_a and c_m respectively, where $c_a, c_m > 0$. It is reasonable to assume that $w > c_a, c_m$, since otherwise the attacker does not have incentive to attack and the defender does not have incentive to monitor. In a resource-constrained network, cost of monitoring (c_m) can be defined as a function of energy consumption with respect to the monitoring activities; cost of attacking (c_a) can be defined as a function of energy consumption with respect to the attack activities.

Table 1: Strategic form of static Bayesian game

	Monitor	Not monitor
Attack	$(1-2\alpha)w - c_a$, $(2\alpha-1)w - c_m$	$w - c_a$, $-w$
Not attack	0, $-\beta w - c_m$	0, 0

(a) Player i is malicious

	Monitor	Not monitor
Not attack	0, $-\beta w - c_m$	0, 0

(b) Player i is regular

In Table 2(a), for the strategy combination (*Attack*, *Not monitor*), defender j's payoff is $-w$, and the malicious type of player i's payoff is his gain of success minus the attacking cost, i.e. $w - c_a$. For the strategy combination (*Attack*, *Monitor*), defender j's payoff is the expected gain of detecting the attack minus the monitoring cost c_m. The expected gain of detecting the attack depends on the value of α, which is $\alpha w - (1-\alpha)w = (2\alpha - 1)w$. Note that $1 - \alpha$ is the false negative rate. In contrast, the malicious type of player i's gain is the loss of defender j, which is $(1 - 2\alpha)w$. Thus the payoff of player i is his gain minus the attacking cost. For the other two strategy combinations, when player i plays *Not attack*, his payoff is always 0. In both cases, defender j's payoff is 0 if he decides not to monitor, and he has a monitoring cost c_m and an expected loss $-\beta w$ due to false alarms if he monitors.

In Table 2(b), the payoff of the regular type of player i is always 0. The payoff of defender j is 0 if he decides not to monitor, and has a monitoring cost c_m and an expected loss due to the false alarm, $-\beta w$, if he monitors.

2.2 Bayesian Nash Equilibrium (BNE) Analysis

Suppose defender j assigns a prior probability μ_0 to player i being malicious. Figure 1 illustrates the extensive form of the static Bayesian game. In the figure, node N represents a "nature" node, who determines the type of player i.

The objective of both players is to maximize their expected payoffs. This implies that we assume that both players are rational. This assumption is a generic assumption for a well-defined game, and it fits in perfectly with the attacker-defender scenario in the sense that the attacker would like to play a Bayesian strategy to minimize his chances of being detected, and the defender would also want to play a Bayesian strategy in order to maximize his chance of detecting attacks without overspending his energy on monitoring. Adopting a non-Bayesian strategy is expected to reduce the players'

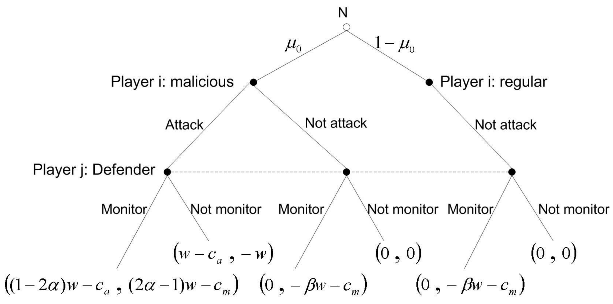


Figure 1: Extensive form of static Bayesian game

payoffs.

In the following, we analyze BNE based on the assumption that μ_0 is a common prior, i.e. player i knows defender j's belief of μ_0.

- If player i plays his pure strategy pair (*Attack* if malicious, *Not attack* if regular), then the expected payoff of defender j playing his pure strategy *Monitor* is

  $$Eu_j(\mathit{Monitor}) = \mu_0((2\alpha-1)w-c_m)-(1-\mu_0)(\beta w+c_m),$$

  and his expected payoff of playing his pure strategy *Not monitor* is

  $$Eu_j(\mathit{Not\ monitor}) = -\mu_0 w.$$

  So if $Eu_j(\mathit{Monitor}) > Eu_j(\mathit{Not\ monitor})$, or if $\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$, then the best response of player j is to play *Monitor*. However, if defender j plays *Monitor*, *Attack* will not be the best response for the malicious type of player i, and he will move on to play *Not attack* instead. Hence, ((*Attack* if malicious, *Not attack* if regular), *Monitor*, μ_0) is not a BNE. However, if $\mu_0 < \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$, the best response for defender j is *Not monitor* and thus ((*Attack* if malicious, *Not attack* if regular), *Not monitor*, μ_0) is a pure-strategy BNE.

- If the malicious type of player i plays his pure strategy *Not attack*, defender j's dominant strategy is to play *Not monitor*, regardless of μ_0. However, if defender j plays *Not monitor*, the best response for the malicious type of player i is to play *Attack*, which reduces to the previous case. So strategy ((*Not attack* if malicious, *Not attack* if regular), *Not monitor*) is not a BNE.

- We previously showed that no pure-strategy BNE exists for the game when $\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$. A mixed-strategy BNE is derived as follows. Let p be the probability with which player i plays *Attack*, and q be the probability with which defender j plays *Monitor*. The expected payoff of defender j playing *Monitor* is

  $$\begin{aligned}Eu_j(\mathit{Monitor}) =& p\mu_0((2\alpha-1)w-c_m)\\ &-(1-p)\mu_0(\beta w+c_m)\\ &-(1-\mu_0)(\beta w+c_m),\end{aligned}$$

  and the expected payoff of defender j playing *Not monitor* is

  $$Eu_j(\mathit{Not\ monitor}) = -p\mu_0 w.$$

  By imposing $Eu_j(\mathit{Monitor}) = Eu_j(\mathit{Not\ monitor})$, we get that the malicious type of player i's equilibrium strategy is to play *Attack* with probability $p^* = \frac{\beta w+c_m}{(2\alpha+\beta)w\mu_0}$. Similarly, By imposing $Eu_i(\mathit{Attack}) = Eu_i(\mathit{Not\ attack})$, we get that defender j's equilibrium strategy is to play *Monitor* with probability $q^* = \frac{w-c_a}{2\alpha w}$. Thus, strategy pair (($p^*$ if malicious, *Not attack* if regular), q^*, μ_0) is a mixed-strategy BNE.

In summary, the static Bayesian game has no pure-strategy BNE if $\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$, but has a mixed-strategy BNE ((p^* if malicious, *Not attack* if regular), q^*, μ_0). That is, if defender j's belief about the maliciousness of player i is high enough ($\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$), a mixed-strategy BNE exists for which defender j plays *Monitor* with probability q^*, and player i plays *Attack* with probability p^* if malicious and plays *Not attack* if regular. We also see that if defender j's belief about the maliciousness of player i is very low ($\mu_0 < \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$), a pure-strategy BNE ((*Attack* if malicious, *Not attack* if regular), *Not monitor*, μ_0) exists. That is, a pure-strategy BNE exists for which defender j plays his pure strategy *Not monitor*, and player i plays his pure strategy *Attack* if malicious and *Not attack* if regular.

Note that the static Bayesian game model is general enough to model most types of attacks in ad hoc networks provided that the IDS is designed to handle these types of attacks. Examples of these kind of attacks supported by the Bayesian model include denial-of-service (DoS) attacks at different network layers (e.g., network layer and transport layer), routing disruption attacks at the network layer, etc. The only exception, is that the Bayesian framework cannot model defense for colluding attacks, due to the game assumption that every node's action is independent of other nodes' actions.

The advantage of using a static Bayesian game model is that instead of applying an always-on IDS monitoring strategy, the defender can implement an efficient monitoring strategy according to his BNE solution that maximizes his expected payoff. One possible drawback in practice is that it may be hard to determine a reasonable prior probability μ_0. In practical applications, the defender can assign μ_0 based on his knowledge of the network environment: if it is a hostile environment, a high value of μ_0 can be assigned.

3. DYNAMIC BAYESIAN GAME

The aforesaid static Bayesian game is a one-stage game, for which the defender maximizes his payoff based on a fixed prior belief about the maliciousness of his opponent. Due to the difficulty of assigning accurate prior probabilities for player i's types, we extend the static Bayesian game to a multi-stage dynamic Bayesian game, where the defender updates his beliefs according to the game evolution.

We assume that the static Bayesian game is repeatedly played in each time period t_k, where $k = 0, 1, ...$ An interval of T seconds may be selected for each stage game. We consider that the game has an infinite horizon because in general any node will not have the information about when his neighboring node leaves the network. The payoffs of the players in each stage game are the same as in the preceding static game, and we assume that there is no discount factor with respect to the payoffs of the players. That is to say that the payoffs remain the same in every stage game. Furthermore, we assume that the players' identities remain consistent throughout the game. This implies that the proposed dynamic game model relies on authentication mechanisms to counteract spoofing, impersonation, and the Sybil [6] attacks. An example of authentication protocol for ad hoc networks is TIK, proposed by Hu et al. in [7].

Continuing with the notations presented in the preceding static game, a *potential* attacker is denoted by i, and a defender is denoted by j. Player i's type θ_i is private information. Defender j's type is regular ($\theta_j = 0$), and it is common knowledge. The players choose actions simultaneously at the beginning of each stage game. The extensive form of each stage game can be represented in a similar manner as for the static Bayesian game (see Figure 1).

We suppose in the beginning of each stage game t_k, the malicious type of player i chooses an action $a_i(t_k)$ in $A_i = \{\textit{Attack, Not attack}\}$, or the regular type of player i chooses his only action *Not attack*; defender j chooses an action $a_j(t_k)$ in $A_j = \{\textit{Monitor, Not monitor}\}$. Similar to the static game, we can define mixed strategies for the constituent static games. For dynamic game, these mixed strategies depend on the history of the game and are denoted as behavior strategies. A behavior strategy specifies a probability distribution over actions at each information set. Specifically, a behavior strategy for player i, denoted by σ_i, is defined as $\sigma_i(a_i(t_k)|\theta_i, \mathbf{h}_i^j(t_k))$, where $\mathbf{h}_i^j(t_k)$ represents the action history profile of player i with respect to his opponent j at the beginning of stage game t_k. We define a behavior strategy for defender j as $\sigma_j(a_j(t_k)|\theta_j, \mathbf{h}_j^i(t_k))$, where $\mathbf{h}_j^i(t_k)$ represents the action history profile of defender j with respect to his opponent i at the beginning of stage game t_k. We define the action history profile of player i with respect to defender j at stage game t_k, $\mathbf{h}_i^j(t_k)$, as a binary vector that contains actions of player i at each stage game t_0, ..., t_{k-1}, which is

$$\mathbf{h}_i^j(t_k) = (a_i^j(t_0), ..., a_i^j(t_{k-1})), \tag{1}$$

where $a_i^j(t_k)$ indicates player i's action with respect to defender j at stage game t_k.

In what follows, to simplify the exposition, we will use an abuse of notation and denote

$$\begin{aligned}
&\sigma_i(a_i(t_k) = \textit{Attack}|\theta_i, \mathbf{h}_i^j(t_k)) = p,\\
&\sigma_i(a_i(t_k) = \textit{Not attack}|\theta_i, \mathbf{h}_i^j(t_k)) = 1-p,\\
&\sigma_j(a_j(t_k) = \textit{Monitor}|\theta_j, \mathbf{h}_j^i(t_k)) = q, \text{and}\\
&\sigma_j(a_j(t_k) = \textit{Not monitor}|\theta_j, \mathbf{h}_j^i(t_k)) = 1-q,
\end{aligned}$$

with the understanding that the mixed strategies p and q for a stage game, will depend on the current information set of the game (the history of the game).

In a stage game t_k, defender j's optimal behavior strategy, depends on his beliefs about the types of player i at the beginning of t_k. In the first stage game t_0, defender j's belief of player i being malicious is characterized by a prior probability μ_0. In the subsequent stages of the dynamic game, defender j can update his beliefs at the end of each stage game based on his observed action of player i and the action history profile of the game.

3.1 Bayesian Updating Rule for Beliefs

We construct a belief updating system for defender j, so that the beliefs of defender j can be updated from stage game t_k to t_{k+1} using Bayes' rule. Specifically, defender j updates his beliefs about the types of his opponent i at the end of each stage game by calculating his posterior beliefs, defined as $\mu_j(\theta_i|a_i(t_k), \mathbf{h}_i^j(t_k))$, where $a_i(t_k)$ represents player i's action at stage game t_k, and $\mathbf{h}_i^j(t_k)$ represents the action history profile of player i with respect to defender j. From Bayes' rule, the posterior beliefs of player j can be computed as follows:

$$\begin{aligned}
&\mu_j(\theta_i|a_i(t_k), \mathbf{h}_i^j(t_k))\\
&\quad = \frac{\mu_j(\theta_i|\mathbf{h}_i^j(t_k))P(a_i(t_k)|\theta_i, \mathbf{h}_i^j(t_k))}{\sum_{\tilde{\theta}_i} \mu_j(\tilde{\theta}_i|\mathbf{h}_i^j(t_k))P(a_i(t_k)|\tilde{\theta}_i, \mathbf{h}_i^j(t_k))},
\end{aligned} \tag{2}$$

where $\mu_j(\tilde{\theta}_i|\mathbf{h}_i^j(t_k)) > 0$, $\mathbf{h}_i^j(t_k) > 0$, and $P(a_i(t_k)|\theta_i, \mathbf{h}_i^j(t_k))$ is the probability that action a_i is observed at this stage of the game, given the type of the opponent and the history of the game.

From Equation (2), we see that, in order to update the belief, at stage game t_k, defender j first needs to "observe" i's action $a_i(t_k)$.

From defender j's point of view, the action (*Attack* or *Not attack*) of player i at each stage game can be observed (detected) by an always-on monitoring system. As described in the preceding static game model, always-on monitoring is not an energy-efficient strategy, instead the defender can use the static game model to derive a better solution. However, although each stage game is considered as a static Bayesian game, this solution will not fit in the stage games of the dynamic model, because belief updating requires the defender to constantly observe the actions of his opponent at each stage game.

To save the energy spent on the IDS, we propose a Bayesian hybrid detection approach that comprises of two monitoring systems: lightweight monitoring system and heavyweight monitoring system. The assumption is that the latter is a more sophisticated IDS which provides more detection power, but consumes more energy. The objective of the hybrid detection approach is to derive efficient monitoring strategies for the two monitoring systems based on a dynamic Bayesian game formulation.

3.2 Bayesian Hybrid Detection

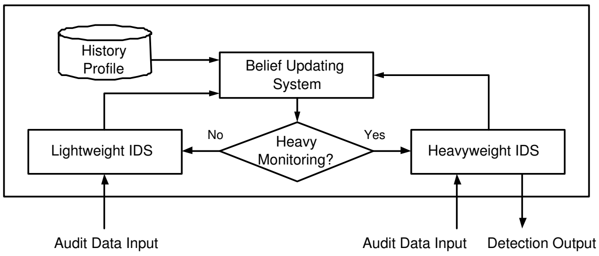


Figure 2: The Bayesian hybrid detection framework.

Figure 2 illustrates the framework of the proposed Bayesian hybrid detection approach. As shown, the decision on setting on or off the heavyweight IDS depends on the output of the belief updating system, which in turn utilizes the information from the lightweight monitoring system and the game history profile as the inputs. In other words, the defender decides whether to activate the heavyweight monitoring system in next stage game based on his updated beliefs of the types of player i at the end of current stage game. The output of the heavyweight IDS can update (or reset) the defender's belief. Note that once the heavyweight IDS is on, the lightweight monitoring is off, so that only one system is active at a time.

To realize the proposed Bayesian hybrid detection approach in practice, we suggest one heavyweight system as the last-resort IDS. We then suggest two lightweight monitoring systems, with one emphasizing on detecting maliciousness of the entire neighborhood (i.e., player i, the defender's opponent, is the entire neighborhood instead of a single node), and the other emphasizing on evaluating neighboring nodes individually (i.e., pairwise attacking/defending node interactions are monitored).

1) One heavyweight monitoring system

For the heavyweight monitoring system, we consider an anomaly based IDS which we previously proposed in [8]. This system employs an association-rule mining technique to find association patterns from a set of packet-level transaction events, which consist of features collected according to Table 2. The IDS builds a normal profile by extracting association rules from training data. Association rules extracted from test data are then compared against the normal profile. Any deviance from the norm is considered as an anomaly rule, which may trigger an intrusion alert accordingly.

Table 2: Cross-layer feature set

Dimension	Value Space
Flow direction (Dir)	SEND, RECV, DROP
Send address (SA)	sa_i, $\forall i \in$ node set S
Destination address (DA)	da_j, $\forall j \in$ node set S
MACFrameType	RTS, CTS, DATA, ACK
RtPktType*	RtDataPkt, RtCtrlPkt

*This feature dimension applies to MAC DATA frame only.

The advantage of this IDS is the ability to identify attack source(s) within one-hop perimeter due to the use of MAC addresses as features for intrusion detection. However, the size of audit data collected from the MAC layer traffic is usually large even for a short time interval. Thus, the normal profile usually contains a large set of rules, even if some aggregation and pruning steps are taken.

2) Two lightweight monitoring systems

Cross-feature analysis system

The cross-feature analysis system is an anomaly detection system that employs the cross-feature mining technique proposed by Huang et al. [9]. This technique explores inter-correlations among features in a feature vector. The details of this system are presented in [10]. Briefly, the cross-feature mining technique is applied to data collected on statistical features, as specified in Table 3. The feature set is defined on the MAC layer data (assume 802.11 MAC), so that the monitoring range of the system is within the neighborhood. A feature vector $\mathbf{f} = \{f_1, f_2, ..., f_k\}$ is a set of quantized feature values collected according to Table 3.

Given a feature vector $\mathbf{f} = \{f_1, f_2, ..., f_k\}$ in a data set, the inter-correlation value of f_i, denoted by r_i, with respect to $\mathbf{f}$ is defined as the conditional probability of f_i. That is, $r_i = p_i(f_i | f_1, f_2, ..., f_{i-1}, f_{i+1}, ..., f_k)$. An overall inter-correlation value of $\mathbf{f}$, denoted by R, is defined as $R = \frac{\sum_i r_i}{k}$. If $R > \theta$, where θ is a decision threshold, $\mathbf{f}$ is classified as a *normal* feature vector. A normal profile consists of a set of normal feature vectors constructed from training data. For test data, each constructed feature vector is tested against the normal profile, and any deviance may trigger an intrusion alert.

Table 3: Statistical feature set

Feature	Value Space	Unit
Time	ignored in classification	second
Network allocator value	continuous	second
Transmit traffic rate	continuous	byte
Receive traffic rate	continuous	byte
Retransmit RTS	discrete	count
Retransmit DATA	discrete	count
Neighbor node count	discrete	count
Forwarding node count	discrete	count

The advantage of this IDS is that the audit data size is dramatically smaller than the one used in the association-rule anomaly detection system. Thus, less time would be spent on both training and testing. Nevertheless, the inclusion of the latter can help to identify the attack source(s).

Note that the cross-feature analysis system is unable to provide attack source information, thus, in the game model, player i represents the entire neighborhood of defender j.

To use the cross-feature analysis system in the dynamic Bayesian game, we consider each sampling interval of the cross-feature analysis system, e.g. 5 seconds, as the time period of a stage game. The action of *Attack* is determined when the feature vector is classified as an abnormal feature vector, and in contrast, the action of *Not attack* is determined when the feature vector is classified as a normal feature vector. Following the determination of player i's action, defender j updates his beliefs about the types of player i. In the next stage game, whether the association-rule analysis (heavyweight monitoring) is activated or not, depends on defender j's posterior belief about player i being malicious, and on the costs associated with each action, according to the game formulation.

Coarse-grained node-to-node analysis system

If interested in evaluating neighboring nodes individually, pairwise attacking/defending node interactions need to be monitored. Because association-rule analysis is not suitable for always-on monitoring due to the massive packet-level transactions in MAC layer and network layer, we propose the following lightweight monitoring system to substitute the cross-feature analysis so that the beliefs of defender i can be updated consistently on consecutive stage games.

Let Γ_j denote the set of neighboring nodes of defender j, where $\Gamma_j \in N$. We consider that a potential attacker i is a neighbor of j, so $i \in \Gamma_j$. We assume i and j have symmetric links, thus $j \in \Gamma_i$. We denote $R_j^i(t_k)$ as the number of packets received at node j from node i. The normalized reception ratio (NRR) of node j from node i for stage game t_k, denoted by $\psi_j^i(t_k)$, is given by

$$\psi_j^i(t_k) = \frac{R_j^i(t_k)}{\sum_{u \neq v} R_{u \in \Gamma_j}^{v \in \Gamma_j}(t_k) + R_j^{v \in \Gamma_j}(t_k)}. \qquad (3)$$

So, NRR of node j reflects the level of inbound traffic rate at node j from node i with respect to the overall traffic rate of the neighborhood of node j. The *Attack* action of player i is determined by applying threshold value τ, where τ is considered as a caution level of node j with respect to player i. That is,

$$a_i(t_k) = \mathit{Attack}, \text{ if } \psi_j^i(t_k) > \tau. \tag{4}$$

From Equations (3) and (4), we see that the complexity of the coarse-grained node-to-node (attacker-to-defender) analysis system is much less than that of the association-rule analysis system which we use it as the heavyweight IDS. In addition, from Table 2, we see that the association-rule analysis includes multiple features (5 feature dimensions and at least 24 features without considering the number of active nodes in the network) for anomaly detection. On the other hand, the coarse-grained node-to-node analysis system only uses one NRR feature. Furthermore, in the association-rule analysis, a normal file usually consists of tens to hundreds association rules. This means that each rule extracted from test data needs to be compared against all the rules in the normal profile. In contrast, the coarse-grained node-to-node analysis system requires only one one comparison at each stage game to determine the action of player i.

The choice of τ influences the performance of coarse-grained node-to-node analysis. Although τ may be determined experimentally by learning the normal traffic pattern in the network, its accuracy is limited by the bursty nature of data traffic. Nonetheless, in our previous work [8], we have shown that using this simple traffic analysis as a preprocessing step for the association-rule analysis leads to a lower false positive rate for the overall system. The drawback of the coarse-grained node-to-node analysis system is that it can only detect inbound traffic attacks such as sleep deprivation, flooding, and some DoS attacks, and it misses outbound traffic attacks such as blackhole and packet dropping attacks.

3.3 Belief Updating in the Presence of Observation Errors

Since the lightweight monitoring system may inevitably produce false positives and false negatives, the "observed" actions may not always accurately reflect the reality. We incorporate the effect of false alarm and misdetection errors for the lightweight IDS, in updating the beliefs by appropriately determining the conditional probabilities $P(a_i(t_k)|\theta_i, \mathbf{h}_i^j(t_k))$. More specifically, denoting with α_p and β_p the detection rate and false positive rate of the lightweight monitoring system, respectively, the above conditional probabilities can be updated as follows:

$$\begin{aligned} &P(a_i(t_k) = \mathit{Attack}|\theta_i = 1, \mathbf{h}_i^j(t_k)) \\ &= \alpha_p \times p + \beta_p \times (1-p), \end{aligned} \tag{5}$$

and

$$\begin{aligned} &P(a_i(t_k) = \mathit{Not\ attack}|\theta_i = 1, \mathbf{h}_i^j(t_k)) \\ &= (1-\alpha_p) \times p + (1-\beta_p) \times (1-p), \end{aligned} \tag{6}$$

and

$$P(a_i(t_k) = \mathit{Attack}|\theta_i = 0, \mathbf{h}_i^j(t_k)) = \beta_p, \tag{7}$$

and

$$P(a_i(t_k) = \mathit{Not\ attack}|\theta_i = 0, \mathbf{h}_i^j(t_k)) = 1 - \beta_p. \tag{8}$$

Note that $1 - \alpha_p$ represent the false negative rate, and $1 - \beta_p$ represent the true negative rate.

We used the notations α_p and β_p in Equations (5)-(8) to differentiate from the detection rate α and the false positive rate β defined in the payoff functions of defender j, which refer to the heavyweight monitoring system.

Provided that defender j can determine player i's action and behavior strategy in each stage game according to the preceding subsections 3.2 and 3.3, defender j can then update his beliefs about the types of player i using Equation (2). Figure 3 demonstrates the convergence of defender j's posterior beliefs under various α_p, β_p, and $\frac{w}{c_a}$. Figures 3(a) and (b) assume the parameters in the payoff functions of the defender are: $\alpha = 0.9$, $\beta = 0.01$, $\frac{w}{c_m} = 1000$ and $\frac{w}{c_a} = 1000$, and Figure 3(c) assumes $\alpha = 0.9$, $\beta = 0.01$, $\alpha_p = 0.8$, $\beta_p = 0.01$. For all three scenarios, defender's prior probability $\mu_0 = \frac{1}{2}$.

From Figure 3(a), we see that the higher α_p is, the faster posterior belief converges to 1. By contrast, Figure 3(b) shows that the lower β_p is, the faster posterior belief converges to 1. In other words, the convergence speed of defender j's posterior belief increases with the detection accuracy of the lightweight monitoring system. From Figure 3(c), we see that the higher the ratio of security value w to the attacking cost c_a is, the faster the convergence speed of defender j's posterior beliefs will be. The ratio of w versus monitoring cost c_m influences the convergence speed in a similar manner.

3.4 Perfect Bayesian Equilibrium (PBE) Analysis

A Dynamic Bayesian game is a multi-stage game with observed actions and incomplete information. In a sequential game, the players best responses are often guided by the threats about certain reactions for other players. For a sequential game with incomplete information, such threats are dependent on the current beliefs, which may change as the game evolves. The concept of PBE defines the proper interaction between users' beliefs about types, given a selection of actions, and the actual strategies. PBE requires that players form a complete system of beliefs about the opponents' types at each decision node that can be reached, update this beliefs according to a Bayes' rule, and the take best response actions using regular Bayesian Nash equilibrium. PBE demands that subsequent play should be optimal for every stage of the game, i.e., it is related to the concept of subgame perfection.

In what follows, we show that our proposed multi-stage attacker/defender game has a PBE. We first show that the proposed multi-stage attacker/defender game satisfies the Bayesian conditions B(i)-B(iv) and equilibrium condition P. The above conditions guarantee that the incomplete-information game has a PBE [5, p333].

Lemma 1: The described multi-stage attacker/defender game satisfies the four Bayesian conditions B(i)-B(iv):

B(i) Posterior beliefs are independent, and all types of player j have the same beliefs, and even unexpected events will not change the independence assumption for the type of the opponents.

B(ii) Bayes' rule is used to update beliefs from $\mu_j(\theta_i|\mathbf{h}_i^j(t_k))$ to $\mu_j(\theta_i|\mathbf{h}_i^j(t_{k+1}))$ whenever possible.

B(iii) The players do not signal what they do not know.

B(iv) All players must have the same belief about the type

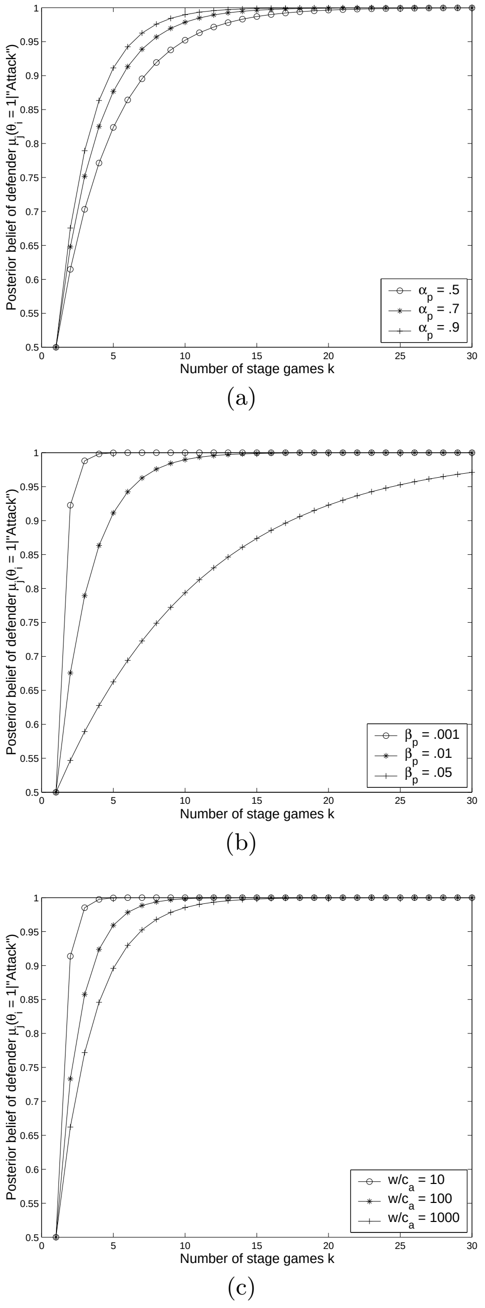


Figure 3: Convergence of defender's posterior beliefs given the observations of a sequence of consecutive *Attack* actions (a) under various α_p, (b) under various β_p, (c) under various ratios of w/c_a.

of another player.

The proof of Lemma 1 is rather trivial because this is a two-player game. Briefly, B(i) is trivially satisfied because defender j has only one type. From the proposed belief updating system, we see that the game satisfied B(ii). Condition B(iii) means $\mu_j(\theta_i = 1|(a_i(t_k), \mathbf{h}_i^j(t_k))) = \mu_j(\theta_i = 1|(\widehat{a}_i(t_k), \mathbf{h}_i^j(t_k)))$, if $a_i(t_k) = \widehat{a}_i(t_k))$. In our attack/defender game context, attacker's signal is part of attack actions, thus B(iii) is satisfied. For condition B(iv), because at any stage game only two players are in the game, and there are no other players influencing the belief updates of the two players.

In essence, Lemma 1 states that each player's belief updating is consistent in every stage game. Based on the assumption of rationality of players, at each stage game, defender j's optimal strategy is to maximize his payoff according to his new beliefs.

Definition 1: In the described multi-stage attacker/defender game, defender j's optimal behavior strategy σ_j^* with respect to his beliefs about player i's type $\mu_j(\theta_i|a_i(t_k), \mathbf{h}_i^j(t_k))$ at stage game t_k satisfies the following relation:

$$u_j((\sigma_i, \sigma_j^*)|\theta_j, \mathbf{h}_i^j(t_k), \mu_j(\cdot)) \geq u_j((\sigma_i, \sigma_j')|\theta_j, \mathbf{h}_i^j(t_k), \mu_j(\cdot)), \tag{9}$$

where σ_j' is an alternative behavior strategy of defender j, and $\mathbf{h}_i^j(t_k)$ is the action history profile of player i with respect to defender j, $\mu_j(\cdot)$ is the abbreviation of $\mu_j(\theta_i|a_i(t_k), \mathbf{h}_i^j(t_k))$, and $u_j(\cdot)$ is the expected payoff of defender j under strategy profile (σ_i, σ_j^*) at stage game t_k.

Analogously, we define potential attacker i's optimal strategy as follows.

Definition 2: In the described multi-stage attacker/defender game, the optimal behavior strategy of a potential attacker i, denoted by σ_i^*, with respect to his beliefs $\mu_i(\theta_j|a_j(t_k), \mathbf{h}_j^i(t_k))$ at stage game t_k satisfies the following condition:

$$u_i((\sigma_i^*, \sigma_j)|\theta_i, \mathbf{h}_j^i(t_k), \mu_i(\cdot)) \geq u_i((\sigma_i', \sigma_j)|\theta_i, \mathbf{h}_j^i(t_k), \mu_i(\cdot)), \tag{10}$$

where σ_i' is an alternative behavior strategy of i, and $\mathbf{h}_j^i(t_k)$ is the action history profile of j with respect to i, $\mu_i(\cdot)$ is the abbreviation of $\mu_i(\theta_j|a_j(t_k), \mathbf{h}_j^i(t_k))$, and $u_i(\cdot)$ is player i's expected payoff under strategy profile (σ_i^*, σ_j) at stage game t_k. Since j has only one type, Equation (10) reduces to

$$u_i((\sigma_i^*, \sigma_j)|\theta_i, \mathbf{h}_j^i(t_k)) \geq u_i((\sigma_i', \sigma_j)|\theta_i, \mathbf{h}_j^i(t_k)). \tag{11}$$

Lemma 2: The described multi-stage attacker/defender game satisfies the equilibrium condition P for multi-stage games of incomplete-information:

(P) For each player x, type θ_x, player x's alternative strategy σ_x', and history $\mathbf{h}(t_k)$, the expected payoff achieved by employing strategy σ_x, denoted by u_x, satisfies the following condition:

$$\begin{aligned} &u_x(\sigma|\mathbf{h}(t_k), \theta_x, \mu(\cdot|\mathbf{h}(t_k))) \\ &\geq u_x((\sigma_x', \sigma_{-x})|\mathbf{h}(t_k), \theta_x, \mu(\cdot|\mathbf{h}(t_k))). \end{aligned} \tag{12}$$

In essence, condition P states that each player's behavior strategy is sequential rational in each stage game. By Definitions 1 and 2, given defender j's belief μ_j, the multi-stage attacker/defender game has a strategy pair $\sigma = (\sigma_i^*, \sigma_j^*)$ that satisfies the above inequality formula, hence condition P is satisfied.

Theorem 1: The described multi-stage attacker/defender game has a perfect Bayesian equilibrium.

Proof: Since the described multi-stage attacker/defender game satisfies the four Bayesian conditions B(i)-B(iv) (Lemma 1) and the equilibrium condition P (Lemma 2), the game has a strategy profile (σ, μ), where $\sigma = (\sigma_i^*, \sigma_j^*)$ is a strategy pair for the two players, and $\mu = (\mu_i(\theta_j|\mathbf{h}_j^i(t_k)), \mu_j(\theta_i|\mathbf{h}_i^j(t_k)))$ is the vector of beliefs for the two players. Note that μ_i is not needed since θ_j's type is common knowledge. By the definition of PBE [5, p333], (σ, μ) is a PBE.

In the subsequent paragraphs, we determine the PBE for each stage game. We analyze the dynamic game as a Bayesian signaling game, in which the actions of potential attacker i signal his type to defender j. Due to the fact that defender j relies on an always-on monitoring system (cross-feature analysis system or lightweight monitoring system) to determine the actions of his opponent i, which is not error free, the equilibrium we seek is always a semi-separating equilibrium. Note that the other two possible equilibria for signaling games, separating and pooling equilibria, do not apply for our scenario [5]. The separating case occurs if the type of the potential attacker i can be perfectly determined after signaling, while in the pooling case, the two types of i cannot be distinguished based on their behavior.

The semi-separating equilibrium, is given by the strategies that maximize both players' payoffs, while none of the players have an incentive to change its strategy. We can see that only a mixed strategy equilibrium exists for each stage game.

To determine this mixed strategy equilibrium we rely on the indifference condition for players' different strategies.

At stage game t_k, if defender j observes that the action of his opponent i was *Attack*, then his expected payoff for playing *Monitor* is

$$\begin{aligned}&Eu_j(a_j(t_k) = Monitor|a_i(t_k) = Attack)\\&= (((2\alpha - 1)w - c_m)p + (-\beta w - c_m)(1 - p))\mu_j(\theta_i = 1|\cdot)\\&+ (-\beta w - c_m)\mu_j(\theta_i = 0|\cdot),\end{aligned} \tag{13}$$

and his expected payoff for playing *Not monitor* conditional on his observation is

$$\begin{aligned}&Eu_j(a_j(t_k) = Not\ Monitor|a_i(t_k) = Attack)\\&= -wp\mu_j(\theta_i = 1|\cdot).\end{aligned} \tag{14}$$

So, player i chooses p^* (the probability with which player i plays *Attack*) to keep defender j indifferent between *Monitor* and *Not monitor*. That is, p^* is derived by setting Equations (13) and (14) equal. Consequently, we have

$$p^* = \frac{\beta w + c_m}{(2\alpha + \beta)w\mu_j(\theta_i = 1|\cdot)}. \tag{15}$$

On the other hand, q^* (the probability with which defender j plays *Monitor*) is selected to keep the malicious type of player i indifferent between his strategies *Attack* and *Not attack*. The indifference condition is given as

$$(((1 - 2\alpha)w - c_a)q + (w - c_a)(1 - q)) = 0, \tag{16}$$

and thus defender j's equilibrium strategy is to choose q^* as

$$q^* = \frac{w - c_a}{2\alpha w}. \tag{17}$$

The PBE for the game is given as $(p^*, q^*, \mu(.))$, with p^*, q^*, $\mu(.))$ given by Equations (15), (17), and (2), respectively.

To see why there is no pure strategy equilibrium for this game, we determine the best response strategy (BR) for both players to be

$$BR_j = \ Monitor \text{ if } p > \frac{\beta w + c_m}{(2\alpha + \beta)w\mu_j(\theta_i = 1|\cdot)}, \tag{18}$$

$$BR_i = \ Attack \text{ if } q < \frac{w - c_a}{2\alpha w}. \tag{19}$$

If (18) holds ⇒ monitor, $q = 1$ ⇒ (19) does not hold ⇒ not attack, $p = 0$ ⇒ (18) does not hold ⇒ not monitor, $q = 0$, ... Using the above argument, we see that there is no pure strategy equilibrium for the analyzed dynamic Bayesian game.

3.5 Advantage of Dynamic Bayesian game

The advantage of implementing the IDS system as a Bayesian hybrid IDS is that it allows to save significant energy (potentially spent on continuously monitoring the network), while minimizing the potential damage inflicted by an undetected attacker. This comes as a result of an interesting property of the equilibrium solution: the monitoring probability does not depend on the current belief of the defender on his opponent's maliciousness, but rather influences the attacker behavior. As indicated by Equation (15), a high belief for the defender on his opponent being malicious results in the attacker drastically reducing his attacks. This is a result of the fact that both the attacker and the defender are rational players, and the costs and beliefs are common knowledge for both players. In practice, the attacker may estimate defender's beliefs according to his observations on defender's actions.

As we described in Section 4.2, in the proposed hybrid detection framework, only one monitoring system is active at a time between heavyweight IDS and lightweight IDS. Thus, if we denote as E_j the energy spent by the defender on the heavyweight IDS and by e_j the energy spent on lightweight monitoring, the savings in energy compared with an always-on heavyweight IDS system are equal to

$$E_s = E_j - (qE_j + (1 - q)e_j) = (1 - q)(E_j - e_j). \tag{20}$$

Note that $E_s > 0$, since $E_j > e_j$. Besides saving energy consumption cost, the use of hybrid detection framework can also reduce the probability of false alarm for the overall equivalent IDS. Our simulation results show that by adding the very simple coarse-grained node-to-node analysis system in front of the association-rule analysis system will reduce the probability of false alarm for the overall equivalent IDS.

4. MULTIPLAYER CONSIDERATION

Both the static and dynamic Bayesian games proposed so far, are two-player games. As we have already mentioned for the cross-feature analysis IDS, the two-player game can also be set up as the defender, against his entire neighborhood. This relaxes the assumption of pairwise interactions in the attacker/defender game.

For our proposed hybrid IDS systems, the defender has also the option to evaluate each of his neighboring nodes individually using the coarse-grained node-to-node analysis system. In general, a maximum degree of uncertainty on the neighboring nodes' types can be reflected by selecting equal prior probabilities for the types of each node. As the game evolves, the defender learns about his neighbors through their past actions, and updates his beliefs accordingly. At each stage of the game, the defender can then determine his equilibrium monitoring strategy based on his highest posteriori belief on maliciousness among his active neighbors. Here, "active" means the nodes who have interactions with the defender.

5. NUMERICAL EXAMPLES

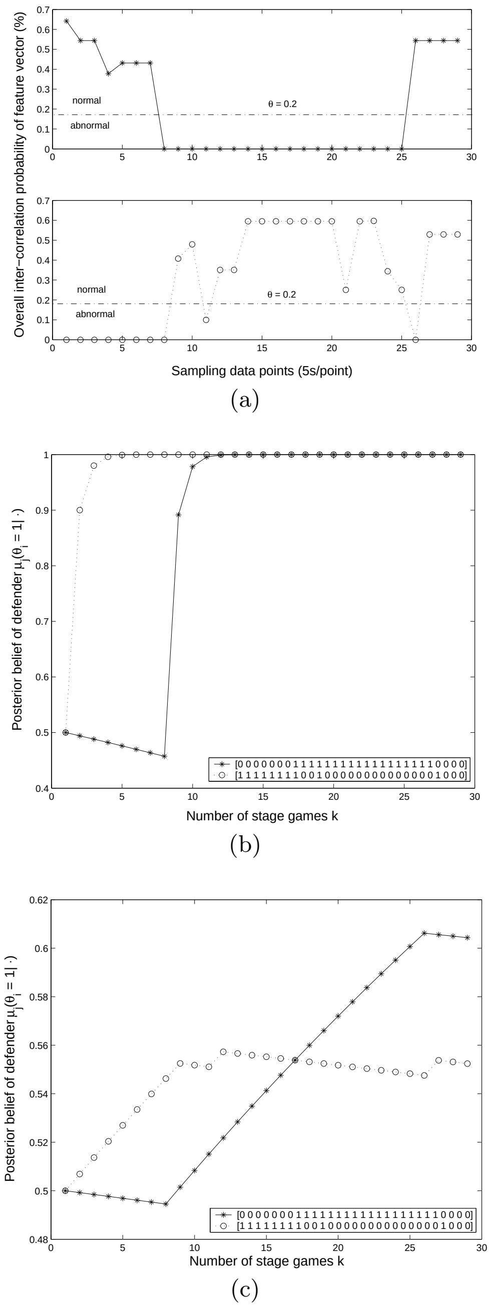
In this section, we provide examples to illustrate the equilibrium achieved for the dynamic Bayesian game. We use the cross-feature analysis to determine actions of a potential attacker in each stage game.

In our previous work [8, 10], we have simulated a network of 500 x 500 square meters on the network simulator ns2 [11] platform, and evaluated the performance of the association-rule analysis system and the cross-feature analysis system separately. We have set the total number of mobile nodes to 30, and the maximum moving speed of a node to 10 m/s. Our simulation results show that the detection rate and false positive rate of the association-rule analysis system against blackhole attack are $\alpha = 91.78\%$ and $\beta = 0.25\%$ respectively, and the detection rate and false positive rate of the cross-feature analysis system are $\alpha_p = 83.33\%$ and $\beta_p = 0.29\%$ respectively. Note that α and β are the parameters in the payoff functions of the defender, while α_p and β_p are used to estimate the potential attacker's behavior strategies as given in Equations (5)-(8).

We first consider a military mobile ad hoc network, which requires high degree of security. For instance, the network must meet stringent confidentiality requirements and must be resistant to DoS attacks. In such circumstances, the security value w is considered very high as compared with the monitoring cost and the attacking cost, i.e. $w >> c_m, c_a$. For illustration purpose, we choose $\frac{w}{c_m} = 1000$ and $c_a = c_m$ (note that, if choosing $c_a < c_m$, then q^* increases to a higher level, and if choosing $c_a > c_m$, then q^* decreases to a lower level).

For this example network, suppose a defending node plays the previously proposed dynamic Bayesian game against *potential* attacker(s). The PBE for the game has the malicious type of player i playing *Attack* with probability $p^* = \frac{0.0019}{\mu_j(\theta_i=1|\cdot)}$, and defender j playing *Monitor* with probability $q^* = 54.42\%$ (here *Monitor* refers to the association-rule analysis system - heavy monitoring). Assume that defender j's prior beliefs for both types of player i are $\frac{1}{2}$, then the first stage game BNE has player i playing *Attack* with probability $p^* = 0.38\%$. This means that the potential attacker (i.e. malicious type of player i) has a very low probability to attack in order to avoid detection. In the subsequent stage games, if defender j's posterior belief for maliciousness updates to a higher level, then p^* is getting even lower for the malicious type of player i.

The second example network is a personal area ad hoc network where each node considers the battery life as the priority requirement. In other words, each defending node



(a)

(b)

(c)

Figure 4: Posterior beliefs of defender j, $\mu_j(\theta_i = 1|\cdot)$ (a) Two sequences of observations of blackhole attack, (b) The corresponding posteriori beliefs of defender j, given $\alpha_p = 83.33\%$, $\beta_p = 0.29\%$, (c) The corresponding posteriori beliefs of defender j, given $\alpha_p = 83.33\%$, $\beta_p = 10\%$.

needs to defend against resource consumption attacks such as sleep deprivation attacks. The security value w of each node may be now represented by his reserved energy. Suppose that $\frac{w}{c_m} = 10$, i.e., if running the heavyweight monitoring system as always-on, the battery energy is cut to $\frac{1}{10}$, and assume that $c_a = c_m$. According to Equations (15) and (17), the PBE of the game has $p^* = \frac{0.0558}{\mu_j(\theta_i=1|\cdot)}$ and $q^* = 49.03\%$. Providing that the defender has equal prior beliefs $(\frac{1}{2})$ on both types of player i, then $p^* = 11.15\%$.

We see that the probability of player i playing *Attack* is 29.35 times higher than one in the previous example, while the probability of defender j playing *Monitor* is lower than the one in the previous example. This means that if the attacker knows that the dynamic game is taken place, then the high security value of the defender will pull back the attacker's probability of attacking, otherwise, the attacker will receive lower payoff which is caused by a successful detection by the defender. On the other hand, because of the defender's high security value, his chances of activate the heavyweight monitoring system also increase. Statistically, the energy saved for using the proposed hybrid detection approach is that instead of turning on the heavyweight monitoring system 100% of the time, the defender only uses it 54.42% of the time, and 49.03% of the time, respectively.

Figure 4 illustrates two sequences of observations of our simulated blackhole attack, and the corresponding posterior beliefs of defender j. At each stage game, the observation of actions is determined by the cross-feature analysis system. Figure 4(a) illustrates the two observation sequences. Each sampling data point represents a feature vector, and if its overall inter-correlation probability is above of the threshold line $\theta = 0.2$, it is then considered as normal feature vector, otherwise it is considered to be abnormal. The binary sequences in Figure 4(b) and (c) corresponds to the observation sequences in Figure 4(a), where bit value 1 represent abnormal or *Attack* action in the corresponding stage game. Figure 4(b) shows that the posterior beliefs converges to 1 quickly due to low false positive rate at each stage game. Once the posterior belief reaches 1, it cannot automatically reduce to a lower level even if the defender observes *Not attack* in the subsequent stage games. This means that the defender has to take defense action, which is to activate association-rule analysis. The output of the association-rule analysis can be used to reset defender's posterior belief. Figure 4(c) shows a scenario in which the defender has a high false alarm rate at each stage game. We can see that if the posterior belief has not yet converged to 1, it is possible to adjust to a lower level based on the new observed actions.

We note that the equilibrium strategy of player i depends on his knowledge of the payoff functions and the updated belief of defender j. So now we seek to determine how robust the strategy selection p is with possible imperfect knowledge on the defender's lightweight monitoring system performance, which may occur in practical scenarios. Figures 5 and 6 present the variation of p with regard to α_p and β_p, respectively. We have assumed that $\alpha_p > \beta_p$. This is a reasonable assumption, since otherwise the lightweight monitoring system is useless. From the two figures, we see that the choice of p is only slightly affected by the values of α_p and β_p, especially for small variation ranges. This implies that the semi-separating equilibrium of the proposed Bayesian game is fairly robust to some imperfect knowledge of the attacker on the performance of the lightweight monitoring system.

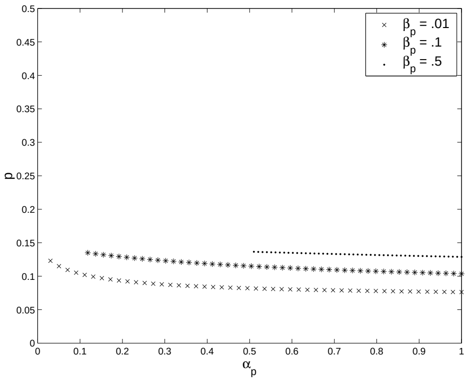


Figure 5: Player i's probability of *Attack* p vs. defender j's lightweight monitoring detection rate α_p.

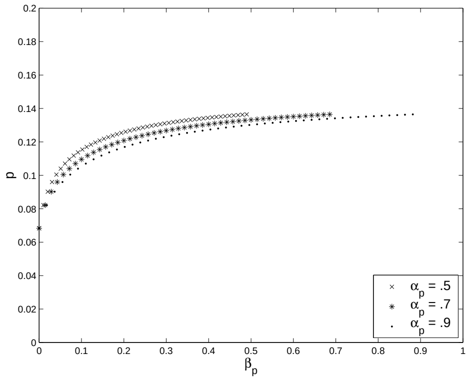


Figure 6: Player i's probability of *Attack* p vs. defender j's lightweight monitoring false alarm rate β_p.

6. RELATED WORK

A game theoretic framework is suitable for modeling security issues such as intrusion prevention and intrusion detection. An example of an intrusion prevention game model is presented in [12], where the authors propose a game theoretic approach to infer attacker intent, objectives, and strategies (AIOS). In the context of intrusion detection, several game-theoretic approaches have been proposed to wired networks, WLANs, sensor networks, and ad hoc networks.

Kodialam and Lakshman [13] have proposed a game theoretic framework to model the intrusion detection game between two players: the service provider and the intruder. A successful intrusion is when a malicious packet reaches the desired target. In the game, the objective of intruder is to choose a particular path between the source node and the target node, and the objective of the service provider is to determine a set of links on which sampling has to be done in order to detect the intrusion. Essentially, the game is formulated as a two-person zero-sum game, in which the service provider tries to maximize his payoff, which is defined by the probability of detection, and on the other hand, the intruder tries to minimize the probability of being detected.

The optimal solution for both players is to play the minmax strategy of the game. The limitation of this game is the assumption of perfect knowledge, which implies the intruder has considerable information about the network and is able to choose the optimal path in order to play the minmax strategy.

In general, using a zero-sum game to model the problem of intrusion detection has a limitation, that is, the cost of intrusion and the cost of detection is assumed to be strictly competitive commodities. This obviously is not true in most cases. For example, in [13], the cost of sampling at multiple links is much higher than the cost of sending a malicious packet on a particular path.

Alpcan and Basar [14] presented a game theoretic approach to intrusion detection in distributed virtual sensor networks, where each agent in the network has imperfect detection capabilities. They model the interaction between the attacker(s) and the IDS as a noncooperative non-zero-sum game with two versions: finite and continuous-kernel versions. In their model, besides the attacker(s) and the IDS, a third "fictitious" player is added to the game to represent the output of the sensor network during a specific attack, which is a fixed probability distribution that is defined as the ratio of the detection probability (i.e. set an alert) at the target sensor to the sum of the detection probabilities of all the sensors in the network. The authors then suggest a cost function to the continuous-kernel security game, which is parameterized by this probability distribution. Nonetheless, because both the attacker and the IDS try to minimize their costs according to the cost function, this implies that both players have knowledge about the probability of detection of every sensor (with respect to the specific attack) in the overall network during the course of the game.

A two-player noncooperative, non-zero-sum game has also been studied by Agah et al. [15] and Alpcan and Basar [16] to address attack-defense problems in sensor networks. Similar to our one-stage attacker/defender game as described in Section 2.1, in their model, each player's optimal strategy depends only on the payoff function of the opponent, and the game is assumed to have complete information. However, as we pointed out earlier, this assumption has limitations in a real network.

Most game-theoretic solutions previously proposed for ad hoc networks focus on modeling cooperation and selfishness of the network (e.g. [17, 18, 19, 20, 21]). In these games, each node choose whether to forward or not forward a packet based on the concern about his cost (energy consumption), his benefit (network throughput), and the collaboration offered to the network by the neighbors. Each of these works try to show that by enforcing cooperation mechanisms, a selfish node not abiding the rules will have low throughput in return from the network. For example, in [17], each node uses the normalized acceptance rate (NAR) to evaluate what action he will choose (i.e. forward or not forward) when he receives a packet. NAR is defined as the ratio of the number of successful relay requests generated by a node, to the number of relay requests made by the node.

In this work, we use dynamic Bayesian game to model the interactions between attacker and defender in ad hoc networks. This allows the two players to choose their optimal strategies according to the action history profile and their beliefs about the types of their opponents, and hence help to overcome the limitations of one-stage static game.

7. CONCLUSION

In this paper, we have proposed a Bayesian game formulation for IDS implementation in wireless ad hoc networks. In these games, each player tries to maximize its payoff: the attacker seeks to inflict the most damage in the network without being detected, while the defender tries to maximize his defending capabilities with a constraint on its energy expenditure for heavy traffic monitoring using IDS, and without complete information on the type of his opponent.

In the proposed static game, the defender always assume fixed prior probabilities about the types of his opponent throughout the entire game period. On the other hand, a more realistic model, the dynamic game, allows the defender to update his belief about his opponent's type based on new observed actions and the game history. We have shown that the static game leads to a mixed-strategy BNE when the defender's belief of player i being malicious is high and to a pure-strategy BNE when the defender's belief of player i being malicious is low. We have also shown that the dynamic game has a mixed-strategy PBE. We have proposed a novel Bayesian hybrid detection approach which uses the dynamic game model to derive equilibrium strategies for both players. We have shown that the equilibrium strategies can preserve energy expenditure, and improve the performance of the hybrid detection approach. Finally, we have shown that, while the equilibrium depends on the malicious node's knowledge on the defender's utility for different actions, and depends on what he thinks about the defender's updated belief, it is fairly robust to the malicious node's imperfect knowledge on the performance of the defender's lightweight monitoring system.

8. REFERENCES

[1] Y. Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147, October 2003.

[2] H. Deng, Q. Zeng, and D.P. Agrawal. SVM-based intrusion detection system for wireless ad hoc networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC'03)*, volume 3, pages 2147–2151, October 2003.

[3] O. Kachirski and R. Guha. Intrusion detection using mobile agents in wireless ad hoc networks. In *Proceedings of the IEEE Workshop on Knowledge Media Networking*, pages 153–158, July 2002.

[4] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 125–134, October 2003.

[5] D. Fudenberg and J. Tirole. *Game Theory.* The MIT Press, Cambridge, Massachusetts, 1991.

[6] J.R. Douceur. The Sybil attack. In *First International Workshop on Peer-to-Peer Systems (IPTPS '02)*, March 2002.

[7] Y-C. Hu, A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *Proc. IEEE INFOCOM 2003*, volume 3, pages 1976–1986, March-April 2003.

[8] Y. Liu, Y. Li, and H. Man. Short paper: A distributed

cross-layer intrusion detection system for ad hoc networks. In *Proc. IEEE/CreateNet the First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005)*, pages 418–420, September 2005.

[9] Y. Huang, W. Fan, W. Lee, and P.S. Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. In *Proc. 23th Int'l Conference on Distributed Computing Systems (ICDCS)*, pages 478–487, May 2003.

[10] Y. Liu, Y. Li, and H. Man. MAC layer anomaly detection in ad hoc networks. In *Proceedings of the sixth IEEE Systems, Man and Cybernetics Information Assurance Workshop*, pages 402–409, June 2005.

[11] J. Broch, D. Maltz, D. Johnson, Y-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, pages 85–97, October 1998.

[12] P. Liu and W. Zang. Incentive-based modeling and inference of attacker intent, objectives, and strategies. In *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pages 179–189, October 2003.

[13] M. Kodialam and T.V. Lakshman. Detecting network intrusions via sampling: A game theoretic approach. In *Proc. IEEE INFOCOM 2003*, volume 3, pages 1880–1889, March-April 2003.

[14] T. Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems. In *Proceeding of the 43rd IEEE Conference on Decision and Control (CDC)*, December 2004.

[15] A. Agah, S.K. Das, K. Basu, and M. Asadi. Intrusion detection in sensor networks: A non-cooperative game approach. In *Proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA'04)*, pages 343–346, August-September 2004.

[16] T. Alpcan and T. Basar. A game theoretic approach to decision and analysis in network intrusion detection. In *Proceeding of the 42nd IEEE Conference on Decision and Control (CDC)*, December 2003.

[17] V. Srinivasan, P. Nuggehalli, C-F. Chiasserini, and R.R. Rao. An analytical approach to the study of cooperation in wireless ad hoc networks. *IEEE Transsactions on Communications*, 4(2):722–733, March 2005.

[18] Y. Xiao, X. Shan, and Y. Ren. Game theory models for IEEE 802.11 DCF in wireless ad hoc networks. *IEEE Radio Communications*, 43(3):S22–S26, March 2005.

[19] J. Cai and U. Pooch. Allocate fair payoff for cooperation in wireless ad hoc networks using Shapley value. In *Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04)*, page 219, April 2004.

[20] P. Nurmi. Modelling routing in wireless ad hoc networks with dynamic Bayesian games. In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference*, pages 63–70, October 2004.

[21] A. Urpi, M. Bonuccelli, and S. Giordano. Modelling cooperation in mobile ad hoc networks: A formal description of selfishness. In *WiOpt'03 Workshop: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, March 2003.