

Coexistence with Malicious Nodes: A Game Theoretic Approach

Wenjing Wang[†], Mainak Chatterjee[†] and Kevin Kwiat[‡]

[†] Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816

[‡] Air Force Research Laboratory, Information Directorate, Rome, NY 13441

Abstract—In this paper, we use game theory to study the interactions between a malicious node and a regular node in wireless networks with unreliable channels. Since the malicious nodes do not reveal their identities to others, it is crucial for the regular nodes to detect them through monitoring and observation. We model the malicious node detection process as a Bayesian game with imperfect information and show that a mixed strategy perfect Bayesian Nash Equilibrium (also a sequential equilibrium) is attainable. While the equilibrium in the detection game ensures the identification of the malicious nodes, we argue that it might not be profitable to isolate the malicious nodes upon detection. As a matter of fact, malicious nodes and regular nodes can co-exist as long as the destruction they bring is less than the contribution they make. To show how we can utilize the malicious nodes, a post-detection game between the malicious and regular nodes is formalized. Solution to this game shows the existence of a subgame perfect Nash Equilibrium and the conditions that achieve the equilibrium. Simulation results and their discussions are also provided to illustrate the properties of the derived equilibria.

I. INTRODUCTION

Game theory [5], [17] has been successfully applied to solve various problems in wireless networks including cooperation enforcement [3], [4], [7], [15], [18], routing protocols [6], [16], [20], [21] and other system design issues [11], [14]. The underlying assumption in most of the existing approaches regard the entities in the network (also called nodes) as selfish and rational. The selfish nodes, governed by their utility functions, only care about their own payoffs and choose corresponding strategies to maximize them. Usually, the payoffs are the benefits a node can derive from other nodes or the network. However, it is possible that there are some nodes whose objective is to cause harm and disorder to the network. These nodes, referred as *malicious* nodes, do not reveal their identities while disrupting network services. The objective of the malicious nodes is to maximize the damage before they are detected and isolated. They are also rational, and their payoff is determined by the amount of damage they cause to the network.

In order to minimize the impact of the malicious nodes, detection mechanism needs to be in place. Thus, a regular node should monitor its surroundings and distinguish a malicious node from a regular one. However, the detection process has challenges. First, monitoring can be costly. To identify the

malice, a regular node has to listen to the channel and/or process the information sent by the nodes being monitored. The listening and processing consume resources of a regular node. Hence, an “always on” monitoring scheme is not efficient even if plausible. Second, the malicious node can disguise itself. To reduce the probability of being detected, a malicious can behave like a regular node and choose longer intervals to attack the network. Third, the randomness and unreliability of the wireless channel bring more uncertainty to the monitoring and detection process.

Nevertheless, identifying the malicious nodes is not the end of the story. Although in most cases, a malicious node is isolated as soon as it is detected, there might be situations where malicious nodes can be kept and made use of. The most straightforward reason for the coexistence is that a malicious node has no idea whether it has been identified or not, and it will continue to operate like a regular node to avoid detection. During this time, i.e., when the malicious node cooperates in disguise, it can be exploited for normal network operations. This “involuntary” help from the malicious node may be valuable, especially when the network resource is limited. As a matter of fact, from the perspective of the malicious nodes, coexistence gives them a longer lifetime in the network and the opportunity to launch future attacks. On the contrary, the regular nodes have a criteria to evaluate the benefit from the malicious nodes. The criteria also determine when to terminate the coexistence and isolate the malicious nodes.

Recently, much work has been done that investigates the interactions between the regular and malicious nodes using game theory. Kodialam *et. al.* formally propose a game theoretic framework to model how a service provider detects an intruder [8]. However, their assumptions of zero-sum game and complete, perfect knowledge have limitations. Agah *et. al.* study the non-zero-sum intrusion detection game in [1]; their results infer the optimal strategies in one-stage static game with complete information. In [13], Liu *et. al.* propose a Bayesian hybrid detection approach to detect intrusion in wireless ad hoc networks. They design an energy efficient detection procedure while improving the overall detection power. [12] models the intention and strategies of a malicious attacker through an incentive-based approach. The importance of the topology on the payoffs of the malicious nodes are investigated in [19]. An interesting flee option for the malicious node is proposed in [10]. In that analysis, a malicious decides to flee when it believes it is too risky to stay in the network. While the approach focuses on how the

Emails: {wenjing, mainak}@eeecs.ucf.edu, kevin.kwiat@rl.af.mil. This research was sponsored by the Air Force Office of Scientific Research (AFOSR) under the federal grant no. FA9550-07-1-0023 and AT&T Graduate Fellowship in Modeling and Simulation. Approved for Public Release; distribution unlimited; 88ABW-2008-1164, 02DEC08.

flee action affects the result of the game, it does not consider the noise in observation.

Our focus in this research is to use game theory to model and analyze the interactions between a malicious node and a regular node. In particular, we formalize the interactions into two cascaded games. The first game, namely *malicious node detection game*, is a Bayesian game with imperfect information. The information is hidden because the malicious node can disguise as a regular node and the actions are hidden due to the noise and imperfect observation. The second game, called *post-detection game*, is played when the regular node knows confidently that its opponent is a malicious node. In the latter game, the regular node observes and evaluates the actions of the malicious node, and decides whether to keep it or isolate it. For both games, we show the existence of equilibria and derive the conditions that achieve them. We also provide simulation study to support the efficiency of the equilibria. The main contributions in this paper can be categorized into two parts.

- We model the malicious node detection game under unreliable channels as a Bayesian game with imperfect monitoring and show a mixed strategy perfect Bayesian Nash Equilibrium is attainable. The strategy profile is also shown to give a sequential equilibrium solution. Results show how the equilibrium strategy profiles are affected by parameters like channel noise, successful attack rate, successful detection rate, attack gain, detection gain, false alarm rate and etc.
- We propose the notion of coexistence after detection in order to utilize the malicious node. A coexistence index is designed to evaluate the helpfulness of a malicious node. We derive the conditions under which a subgame perfect Nash Equilibrium is achieved. Through simulation, we also show how the malicious node can be used to improve the network throughput and extend network lifetime.

The rest of the paper is organized as follows. In Section II, we introduce and solve the Bayesian game of malicious node detection. Section III presents the post-detection game and discusses how malicious and regular nodes can coexist after detection. Simulation results are presented in Section IV that illustrate our findings. The last section concludes the paper.

II. DETECTING MALICIOUS NODES UNDER UNRELIABLE CHANNELS

A. Network Model

We consider a wireless network consisting of a fixed number of nodes. The types of the nodes can be either *Regular* or *Malicious*. For a regular node, its actions are rational and are governed by an underlying utility function. A rational action may not be cooperative if such cooperation is not profitable. A regular node is selfish (i.e., acts towards its own interest); however, it never brings malice to the network. On the other hand, a malicious node aims to hamper, disturb, and even attack the network. Although the actions of a malicious node is also determined by certain utility functions, such functions are designed to bring damages to the network.

Despite the two types of nodes, the identity (type) of a malicious node is not directly revealed to others. Instead, the types can only be estimated or conjectured through observing actions. To identify the attacks and malicious nodes in the network, a regular node can monitor the actions of others. However, such monitoring is costly (e.g., consumes the receivers' own resource) and a node cannot afford to monitor all the time. Moreover, the observations might not be accurate because of the noise, e.g., wireless channel loss. Thus, the regular nodes do not monitor the network all the time and during those times, attacks cannot be identified.

To simplify the analysis, our research focuses on the packet forwarding process. We assume that node i , or the sender node, has a packet to send to node j , or the receiver node. If the sender node is regular, it only takes the action "Forward". If the sender node is malicious, it can choose to "Attack" with a risk of being identified or "Forward" (not attack) to disguise. We further assume that time is divided into slots and nodes take their actions within each slot.

B. Game Model

To abstract the interactions among the nodes, we consider a two-player game played by the sender node i and the receiver node j . The types of these nodes, θ_i and θ_j , are private information. Since the type of each player is hidden, and the observation is not accurate, it is a Bayesian game with imperfect information [17].

To model the process of detecting the malicious nodes in the network, we apply a special category of Bayesian game called the signaling game. A *signaling game* is played between a sender and a receiver. The sender has a certain type and a set \mathcal{M} of available messages to be sent. Based on its knowledge on its own type, the sender chooses a message from \mathcal{M} and sends it to the receiver. However, the receiver does not know the type of the sender and can only observe the message but not the type. Through observation, the receiver then takes an action in response to the message it observed. In the malicious node detection game, the sender, node i can be either regular $\theta_i = 0$ or malicious, $\theta_i = 1$. The receiver, node j is always a regular node, i.e., $\theta_j = 0$.

The action profiles a_i available to node i are based on its type. For $\theta_i = 0$, $a_i = \{Forward\}$. For $\theta_i = 1$, $a_i = \{Attack, Forward\}$. The receiver node j has the option to monitor if node i is attacking or not, thus $a_j = \{Monitor, Idle\}$.

To further construct the game, we define the following values. Let g_A be the payoff of a malicious node if it successfully attacks. The cost associated with such an attack is c_A . For the receiver node j , the cost of monitoring is c_M and 0 if it is idle. Hence, for the action profile $(a_i, a_j) = (Attack, Idle)$, the net utility for a successful attacking node i is $g_A - c_A$, the loss for node j is $-g_A$ due to the attack. Similarly, if the action profile is $(a_i, a_j) = (Attack, Monitor)$, the attacking malicious node i losses $g_A + c_A$, and the net gain for node j is $g_A - c_M$. However, if a malicious node chooses not to attack, the cost to forward a packet is c_F , which is the same cost to a regular sender

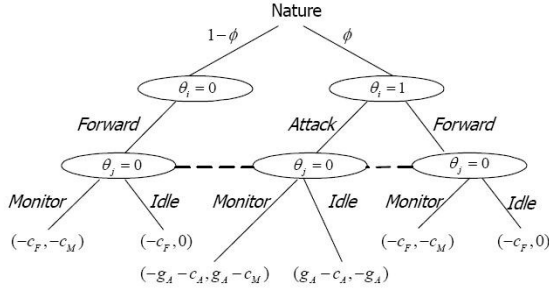


Fig. 1. Stage malicious node detection game tree.

node. Based on the types of node i and node j , the payoff matrices are presented in Table I.

In addition, in our model, we introduce p_e as the channel loss rate. The channel unreliability implies that monitoring can be accurate with probability $1 - p_e$. We also denote γ as the attack success rate.

		(a) $\theta_i = 1$, malicious sender	
		Node j	
Node i	Attack	Monitor	Idle
		Forward	$-g_A - c_A$ $-c_F$
		(b) $\theta_i = 0$, regular sender	
		Node j	
Node i	Forward	Monitor	Idle
		$-c_F$	$-c_M$

TABLE I

PAYOFF MATRIX OF TWO PLAYER MALICIOUS NODE DETECTION GAME.

C. Equilibrium analysis for the stage game

We begin our analysis on the malicious node detection game from the extensive form of the static Bayesian game as illustrated in Figure 1. We consider the type determination of node i when $\theta_i = 1$ happens with probability ϕ . To solve this game, we are interested in finding the possible *Bayesian Nash Equilibrium* (BNE). In a static Bayesian game, the BNE is the Nash Equilibrium given the beliefs of both nodes. In our case, node i knows for sure that for node j , $\theta_j = 0$, however, node j 's belief about node i is that $\theta_i = 1$ with probability ϕ .

First, let us consider pure strategies only. Based on θ_i , the pure strategies available for node i are $\sigma_i = \{(\text{Attack if } \theta_i = 1, \text{Forward if } \theta_i = 0), \text{Forward } \forall \theta_i\}$. For node j , the strategy set is $\sigma_j = \{\text{Monitor}, \text{Idle}\}$. To find the BNE, we let σ_i and σ_j play with each other and derive the conditions under which neither node can increase its utility by unilaterally changing its strategy.

LEMMA 1: In the malicious node detection game, there is a malice belief threshold ϕ_0 , such that no pure strategy BNE exists if $\phi > \phi_0$.

Proof: We start by eliminating a trivial pure strategy pair (*Forward* $\forall \theta_i$ *Monitor*). From Table I(a), we know that for both nodes, they can improve their payoffs by deviating from the strategy pair. We further analyze the following two cases.

Case 1: $\sigma_i = (\text{Attack if } \theta_i = 1, \text{Forward if } \theta_i = 0)$. For node j , if $\sigma_j = \text{Monitor}$, the expected payoff is

$$u_j(\text{Monitor}) = (g_A - c_M)\phi(1 - p_e) - \phi p_e[\gamma(g_A + c_M) + (1 - \gamma)c_M] - (1 - \phi)c_M \quad (1)$$

where each term represents monitoring the attack successfully, failing to monitor the attack, and node i is regular respectively. If $\sigma_j = \text{Idle}$, the expected payoff is

$$u_j(\text{Idle}) = -\phi\gamma g_A \quad (2)$$

If (2) > (1), the dominant strategy for node j is *Idle*. Correspondingly, for node i , the best response would be (*Attack if* $\theta_i = 1$, *Forward if* $\theta_i = 0$). Thus $(\sigma_i, \sigma_j) = \{(\text{Attack if } \theta_i = 1, \text{Forward if } \theta_i = 0), \text{Idle}\}$ is a BNE under the condition that $\phi < \frac{c_M}{(1-p_e)(1+\gamma)g_A}$. If (2) < (1), or $\phi > \frac{c_M}{(1-p_e)(1+\gamma)g_A}$, the dominant strategy for node j is *Monitor*, however, the best response to *Monitor* for node i is *Forward* $\forall \theta_i$. Hence $(\sigma_i, \sigma_j) = \{(\text{Attack if } \theta_i = 1, \text{Forward if } \theta_i = 0), \text{Monitor}\}$ is not a BNE under the condition that $\phi > \frac{c_M}{(1-p_e)(1+\gamma)g_A}$.

Case 2: $(\sigma_i, \sigma_j) = \{(\text{Forward } \forall \theta_i, \text{Idle})\}$. If node j chooses not to monitor, the best response for node i is to *Attack* if $\theta_i = 1$. This will lead to the previous case when $\phi < \frac{c_M}{(1-p_e)(1+\gamma)g_A}$. Therefore, there is no BNE if $(\sigma_i, \sigma_j) = \{(\text{Forward } \forall \theta_i, \text{Idle})\}$.

To sum up, the pure strategy BNE exists if and only if $\phi < \frac{c_M}{(1-p_e)(1+\gamma)g_A}$. The equilibrium strategy profile is $(\sigma_i, \sigma_j) = \{(\text{Attack if } \theta_i = 1, \text{Forward if } \theta_i = 0), \text{Idle}\}$. In other words, we can find $\phi_0 = \frac{c_M}{(1-p_e)(1+\gamma)g_A}$, such that no pure strategy BNE exists if $\phi > \phi_0$. \square

Although pure strategy BNE exists, it is not practical because the equilibrium requires node j to be *Idle* at all times, and hence the malicious nodes cannot be detected. It is also called *Pooling Equilibrium* [17] in which the receiver has no clue about sender's type. Therefore, it is desirable to seek a mixed-strategy BNE, and obviously, such BNE exists when $\phi > \phi_0$.

Let us denote p as the probability with which node i of type $\theta_i = 1$ plays *Attack* and q as the probability with which node j plays *Monitor*. To find the mixed strategy BNE of this game, we need to find the values of p and q such that neither node i nor j can increase payoff by altering the actions. For the mixed strategy played by node i , the payoff of node j playing *Monitor* is

$$\begin{aligned} u_j(\text{Monitor}) &= \phi p[\gamma(g_A - c_M)(1 - p_e) + (1 - \gamma)(1 - p_e)(g_A - c_M) \\ &\quad - (1 - \gamma)p_e c_M - \gamma p_e(g_A + c_M)] \\ &\quad - (1 - p)\phi c_M - (1 - \phi)c_M \\ &= \phi p[g_A - g_A p_e(1 + \gamma)] - c_M. \end{aligned} \quad (3)$$

If node j plays *Idle*,

$$u_j(\text{Idle}) = -p\gamma\phi g_A. \quad (4)$$

Thus, in the mixed BNE strategy, $u_j(\text{Monitor}) = u_j(\text{Idle})$. Thus $p = \frac{c_M}{\phi g_A(1+\gamma)(1-p_e)}$. Similarly, when node j

plays the mixed strategy, the payoff of node i playing *Attack* is

$$\begin{aligned} u_i(\text{Attack}) &= -(g_A + c_A)(1 - p_e)q + (g_A - c_A)\gamma(1 - q) \\ &\quad + (g_A - c_A)\gamma qp_e - c_A(1 - \gamma)p_e q \\ &\quad - c_A(1 - q)(1 - \gamma) \\ &= qg_A(p_e - 1)(1 + \gamma) + g_A\gamma - c_A. \end{aligned} \quad (5)$$

When node i plays *Forward*,

$$u_i(\text{Forward}) = -c_F. \quad (6)$$

Hence, to obtain q , $u_i(\text{Attack}) = u_i(\text{Forward})$, and $q = \frac{g_A\gamma - c_A + c_F}{g_A(1 - p_e)(1 + \gamma)}$.

To sum up the analysis, we state the following lemma.

LEMMA 2: The malicious node detection game has a mixed strategy BNE when $\sigma_i, \sigma_j = \left\{ \begin{array}{l} \text{Attack with } \frac{c_M}{\phi g_A(1 + \gamma)(1 - p_e)} \text{ if } \theta_i = 1, \\ \text{Forward if } \theta_i = 0, \\ \text{Monitor with } \frac{g_A\gamma - c_A + c_F}{g_A(1 - p_e)(1 + \gamma)} \end{array} \right\}$, given $\phi > \phi_0$.

Lemmas 1 and 2 provide us with the conditions under which BNE can be attained. One of the conditions is the belief of malice threshold ϕ_0 . As suggested in Lemma 1, this threshold is related to the channel reliability $(1 - p_e)$, attack success rate (γ) and detection gain (g_A/c_M) . In the pure strategy BNE, node i always attacks and the belief of node j on node i 's malice is very low since the detection gain is usually very large as $p_e, \gamma \in [0, 1]$. However, when the belief grows and eventually exceeds the threshold, the mixed strategy BNE requires node i to be less aggressive in attacking. In other words, the equilibrium implies node i should know about node j 's belief when making the decision. When node j is absolutely sure about node i 's type, node i 's equilibrium attack probability drops to the value of the belief threshold.

D. Belief update and dynamic Bayesian games

So far, the analysis on the malicious node detection stage game has shown that the equilibrium is associated with node j 's belief on node i 's type. However, the difficulty lies in the assignment of the belief as a priori information available to node j . Thus, it is desirable that this belief can be accurately presented and dynamically updated. We apply dynamic Bayesian game theory to discuss how the belief is updated.

We assume that the static malicious node detection game is repeatedly played at every time slot, and we consider the infinite repeated game without discounting (i.e., payoffs in every stage/slot have equal weight). In addition to the notation defined in the stage game, we introduce $\mu_j^{(t)}(\theta_i = \tilde{\theta}_i)$ as the belief node j holds about $\theta_i = \tilde{\theta}_i$. Since node j is always a regular node, $\mu_j^{(t)}(\theta_j = 0)$ for all $t > 0$. We further define $a_i(t)$ as the action node i plays at t^{th} stage. Node j may monitor node i 's actions through the observed signal $\hat{a}_i(t)$. The reasons for the discrepancy between $a_i(t)$ and $\hat{a}_i(t)$ are the observation error caused by the channel unreliability and the false alarm rate (α) caused by the inaccuracy and limitation in the detection of node j .

Based on Bayes' theorem, we construct our belief update rule. If node j is continuously monitoring, its belief on θ_i can be calculated with the belief it holds at the immediate previous stage and the actions it observed. We write the belief at the $(t + 1)^{\text{th}}$ stage as:

$$\mu_j^{(t+1)}(\theta_i) = \frac{\mu_j^{(t)}(\theta_i)P(\hat{a}_i(t)|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_j^{(t)}(\tilde{\theta}_i)P(\hat{a}_i(t)|\tilde{\theta}_i)}, \quad (7)$$

where Θ is the space of all possible values θ_i can take; in our case $\Theta = \{0, 1\}$.

For each of the terms in (7), we have the following equations.

$$P(\hat{a}_i(t) = \text{Attack}|\theta_i = 1) = p(1 - p_e) + (1 - p)\alpha \quad (8)$$

$$P(\hat{a}_i(t) = \text{Attack}|\theta_i = 0) = \alpha \quad (9)$$

$$P(\hat{a}_i(t) = \text{Forward}|\theta_i = 1) = pp_e + (1 - p) + (1 - \alpha) \quad (10)$$

$$P(\hat{a}_i(t) = \text{Forward}|\theta_i = 0) = (1 - p)\alpha. \quad (11)$$

Since node j does not monitor node i 's actions at every stage, when node j is not monitoring, its belief remains the same at the next stage. Thus, (7) is revised as:

$$\mu_j^{(t+1)}(\theta_i) = q \frac{\mu_j^{(t)}(\theta_i)P(\hat{a}_i(t)|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_j^{(t)}(\tilde{\theta}_i)P(\hat{a}_i(t)|\tilde{\theta}_i)} + (1 - q)\mu_k^{(t)}(\theta_i). \quad (12)$$

The concept of *belief system* is hence introduced to describe the aforementioned belief building and updating process. A belief system is a function that assigns each information set¹ a probability distribution over the histories in that information set [17]. Although in our discussions above, we did not explicitly state how history is accounted for in (7) and (12), it is easy to observe that every updated belief is determined by the actions node j observes in the current stage and the belief it holds. The beliefs are further determined by the actions in the previous stages and it can be backtracked to the initial belief and the subsequent actions. Thus, the current belief and observed action can fully represent the histories in the information sets, and those information sets can be reached with positive probabilities if the strategies are carefully designed.

With the belief system, the games are played in a sequential manner. As the game evolves, neither nodes can stick to the very same strategy at every stage to yield the most payoffs. Thus, the best response strategies are dependent on the current beliefs held by the nodes. Perfect Bayesian Equilibrium (PBE) can be applied to characterize the aforementioned dependency. In PBE, the belief system is updated by Bayes' rule. PBE also demands that the optimality of subsequent play given the belief. Next, we show how to construct a PBE in the dynamic malicious node detection game.

¹An information set is a set of all the possible moves that could have taken place in the game so far, for a particular player, given what that player has observed. In an imperfect information game, an information set contains all possible states in the history, e.g., in Figure 1, the dotted lines show the information set available to node j .

We first show the existence of a mixed strategy equilibrium and then argue the infeasibility of the pure strategy equilibrium. Consider at an arbitrary stage k of the game; we denote $p^{(k)}$ as the probability node i of type $\theta_i = 1$ plays *Attack*, $q^{(k)}$ as the probability node j plays *Monitor*. In the equilibrium, $u_i^{(k)}(\text{Attack}) = u_i^{(k)}(\text{Forward})$ and $u_j^{(k)}(\text{Monitor}) = u_j^{(k)}(\text{Idle})$. In particular,

$$\begin{aligned} u_i^{(k)}(a_i^{(k)} = \text{Attack} | a_j^{(k)} = \text{Monitor}) = \\ -(g_A + c_A)(1 - p_e)q^{(k)} + (g_A - c_A)\gamma(1 - q^{(k)}) \\ + (g_A - c_A)\gamma q^{(k)} p_e - c_A(1 - \gamma)p_e q^{(k)} \\ - c_A(1 - q^{(k)})(1 - \gamma) \end{aligned} \quad (13)$$

$$u_i^{(k)}(a_i^{(k)} = \text{Forward} | a_j^{(k)} = \text{Monitor}) = -c_F. \quad (14)$$

$$\begin{aligned} u_j^{(k)}(a_j^{(k)} = \text{Monitor} | a_i^{(k)} = \text{Attack}) = \\ \mu_j^{(k)}(\theta_i = 1)p^{(k)}[\gamma(g_A - c_M)(1 - p_e) \\ + (1 - \gamma)(1 - p_e)(g_A - c_M) - (1 - \gamma)p_e c_M \\ - \gamma p_e(g_A + c_M)] - (1 - p^{(k)})\mu_j^{(k)}(\theta_i = 1)c_M \\ - \mu_j^{(k)}(\theta_i = 0)c_M \end{aligned} \quad (15)$$

$$\begin{aligned} u_j^{(k)}(a_j^{(k)} = \text{Idle} | a_i^{(k)} = \text{Attack}) = \\ -p^{(k)}g_A\gamma\mu_j^{(k)}(\theta_i = 1). \end{aligned} \quad (16)$$

The solutions to the above equations are

$$p^{(k)} = \frac{c_M}{\mu_j^{(k)}(\theta_i = 1)g_A(1 + \gamma)(1 - p_e)} \quad (17)$$

$$q^{(k)} = \frac{g_A\gamma - c_A + c_F}{g_A(1 - p_e)(1 + \gamma)}. \quad (18)$$

What $p^{(k)}$ and $q^{(k)}$ suggest is an equilibrium profile $(\sigma_i^{(k)}, \sigma_j^{(k)})$. This profile shows the sequential rationality [5], [17], that is, each node's strategy is optimal whenever it has to move, given its belief and the other node's strategy. In other words, for any alternative strategies $\sigma_i'^{(k)}$ and $\sigma_j'^{(k)}$,

$$\begin{aligned} u_i^{(k)}((\sigma_i^{(k)}, \sigma_j^{(k)}) | \theta_i, a_i(t), \mu_j^{(k)}(\theta_i)) \geq \\ u_i^{(k)}((\sigma_i'^{(k)}, \sigma_j^{(k)}) | \theta_i, a_i(t), \mu_j^{(k)}(\theta_i)) \end{aligned} \quad (19)$$

$$\begin{aligned} u_j^{(k)}((\sigma_i^{(k)}, \sigma_j^{(k)}) | \theta_i, \hat{a}_i(t), \mu_j^{(k)}(\theta_i)) \geq \\ u_j^{(k)}((\sigma_i^{(k)}, \sigma_j'^{(k)}) | \theta_i, \hat{a}_i(t), \mu_j^{(k)}(\theta_i)) \end{aligned} \quad (20)$$

Besides sequential rationality, a PBE also demands that the belief system satisfies the Bayesian conditions [5].

DEFINITION 1: ([5], p331-332) The Bayesian conditions defined for PBE are

B(i): Posterior beliefs are independent. For history $h^{(t)}, \mu_i(\theta_i | \theta_i, h^{(t)}) = \prod_{j \neq i} \mu_i(\theta_j | h^{(t)})$.

B(ii): Bayes' rule is used to update beliefs whenever possible.

B(iii): Nodes do not signal what they do not know.

B(iv): Posterior beliefs are consistent for all nodes with a common joint distribution on θ given $h^{(t)}$.

Our proposed belief system satisfies the Bayesian conditions. B(i) is satisfied because $\theta_j = 0$ all the time. Eqn. (7) is derived from Bayes' rule, and hence B(ii) is also satisfied.

B(iii) is fulfilled because node i 's signal is determined by its action and if $a_i(k) = \hat{a}_i(k)$, $\mu_j(\theta_i | a_i(k), h_j^{(k)}) = \mu_j(\theta_i | \hat{a}_i(k), h_j^{(k)})$. B(iv) is trivial in our game because no third player exists.

The analysis on Bayesian conditions and sequential rationality serves as the proof of the following theorem.

THEOREM 1: The dynamic malicious node detection game has a perfect Bayesian equilibrium that can be attained with strategy profile $(\sigma_i^{(k)}, \sigma_j^{(k)}) = (p^{(k)}, q^{(k)})$.

Remark 1: The infeasibility of pure strategy PBE is proved as follows: If node i attacks, the best response for node j is *Monitor*, which makes node i non-profitable to play *Attack*. If node i plays *Forward*, $p^{(k)} = 0$, the best response for node j is *Idle* (i.e., $q^{(k)} = 0$). However, the sequential rationality requires $q^{(k)} \geq \frac{g_A\gamma - c_A + c_F}{g_A(1 - p_e)(1 + \gamma)}$, which leads to a contradiction. Therefore, no pure strategy PBE exists in the dynamic malicious node detection game. It is noted that the infeasibility of the pure strategy PBE in the dynamic settings should not be confused with the existence of a pure strategy BNE in a static game because the pure strategy BNE in a static game is always an artifact.

Remark 2: The proved PBE can be further refined to *Sequential Equilibrium* [9]. In the sequential equilibrium, the Bayesian conditions are extended as *belief sensibility* and *consistency*. The belief sensibility requires the information sets can be reached with positive probabilities (μ) given the strategy profile σ . The consistency demands an assessment (σ, μ) should be a limit point of a sequence of the mixed strategies and associated sensible beliefs, i.e., $(\sigma, \mu) = \lim_{n \rightarrow \infty} (\sigma^n, \mu^n)$. In our game, belief sensibility is satisfied because our proposed belief system updates the beliefs according to Bayes' rule and it assigns a positive probability to each of the information set. Theorem 8.2 in [5] states that in incomplete information multi-stage games, if neither player has more than 2 types, Bayesian condition is equivalent to belief consistency requirement. In our game, $\theta_i = 0, 1, \theta_j = 0$, and hence consistency is fulfilled. Together with the sequential rationality, the PBE in our game is also a sequential equilibrium. Since every finite extensive-form game has at least one sequential equilibrium, which is a refinement to PBE, it also implies the existence of PBE in our game.

III. POST-DETECTION GAME AND COEXISTENCE

In the previous section, we have discussed how to update node j 's belief system based on Bayes' rule. It is natural that through observation, although imperfect at every stage game, node j can accumulate a better estimation about θ_i . Eventually, after repeated monitoring, there will be a stage at which node j can predict with confidence whether node i is regular or malicious.

A. The post-detection game

Traditionally speaking, after node j has identified node i as a malicious node, it will try to report and isolate node i immediately to prevent future attacks. However, there are also situations where "isolation" may not be a good choice.

Let us consider a wireless network which operates on a limited resource budget. In order to prolong the lifetime of the network, every regular node has to be economical towards packet forwarding. Hence, if a malicious node can be used to handle some of the traffic, it is beneficial not to isolate it.

However, there is a trade-off between how much benefit a malicious node can bring and what damage it can do. We denote n_F and n_A as the number of successful forwarding actions and number of attacks taken by a malicious node. Recall the cost of forwarding is c_F and the loss due to an attack to the network is g_A . Thus, for a regular node, if it observes that the total saving due to forwarding ($n_F c_F$) a malicious node contributes is greater than the total cost due to its attack ($n_A g_A$), then keeping that node in the network is profitable.

To further analyze the conditions under which a malicious node can be kept and coexist with the regular ones, we formally define the post detection game. The game has two players: node i and node j , both nodes know the types of their opponent, i.e., node j knows that node i is malicious but has not taken any action to isolate it. Thus, $\theta_i = 1$, $\theta_j = 0$. The actions available for node i is $a_i = \{Attack, Forward\}$, while the actions for node j is $a_j = \{Monitor, Idle\}$. When node j monitors, it keeps a record of what node i has done since the beginning of the game. It also calculates a coexistence index $\mathcal{C}_i = \hat{n}_F c_F - \hat{n}_A g_A$ for node i , where \hat{n}_F is the observed number of forwarding actions and \hat{n}_A is the observed number of attacks. If \mathcal{C}_i falls under a certain threshold τ , node j will isolate node i and terminate the post-detection game because keeping node i is no longer beneficial. If $\mathcal{C}_i \geq \tau$, the game will be played in a repeated manner. The payoff matrix for the post-detection game is the same as the detection game for $\theta_i = 1$ as was shown in Table I(a).

B. Searching for a coexistence equilibrium

Let us explore the strategies that both nodes can take to reach the equilibrium of coexistence. To avoid confusion, we denote p^* and q^* as the probability node i plays *Attack* and node j plays *Monitor* respectively. It is noted that these probabilities are different from the ones we obtained in Section II-D.

We first derive the Nash Equilibrium using indifference conditions. Suppose the post-detection game is played at t^{th} repetition, i.e., subgame t . The expected payoff for player j playing *Monitor* is

$$\begin{aligned} u_j^{(t)}(Monitor) &= \{p^*[\gamma(g_A - c_M)(1 - p_e) \\ &+ (1 - \gamma)(1 - p_e)(g_A - c_M) - (1 - \gamma)p_e c_M \\ &- \gamma p_e(g_A + c_M)]\} \Pr(\mathcal{C}_i \geq \tau) \\ &+ (g_A - c_M)p^*(1 - p_e) \Pr(\mathcal{C}_i < \tau) - (1 - p^*)c_M \\ &= [g_A(1 - p_e + \gamma p_e) - c_M]p^* \Pr(\mathcal{C}_i \geq \tau) \\ &+ (g_A - c_M)p^*(1 - p_e) \Pr(\mathcal{C}_i < \tau) - (1 - p^*)c_M \end{aligned} \quad (21)$$

If node j plays *Idle*, the expected payoff is always

$$u_j^{(t)}(Idle) = -p^* \gamma g_A. \quad (22)$$

Thus, the indifference condition require $u_j^{(t)}(Monitor) = u_j^{(t)}(Idle)$, and hence p^* is obtained as in (23) on next page.

Similarly, we can apply the indifference condition to node i as:

$$\begin{aligned} u_i^{(t)}(Attack) &= q^* \{-(g_A + c_A)(1 - p_e) \Pr(\mathcal{C}_i < \tau) \\ &+ (1 - p_e)[(g_A - c_A)\gamma - c_A(1 - \gamma)] \Pr(\mathcal{C}_i \geq \tau) \\ &+ (g_A - c_A)\gamma p_e - c_A(1 - \gamma)p_e\} \\ &- (1 - q^*)[c_A(1 - \gamma) - (g_A - c_A)\gamma] \\ &= q^* \{-(g_A + c_A)(1 - p_e) \Pr(\mathcal{C}_i < \tau) \\ &+ (g_A\gamma - c_A)[(1 - p_e) \Pr(\mathcal{C}_i \geq \tau) + p_e]\} \\ &+ (1 - q^*)(g_A\gamma - c_A). \end{aligned} \quad (24)$$

$$u_i^{(t)}(Forward) = -c_F. \quad (25)$$

Therefore, q^* can be expressed as (26) on next page.

The problem is then reduced to obtaining the probability distribution of \mathcal{C}_i . Let us assume at the beginning of the post-detection game $\mathcal{C}_i = c_0 \geq \tau$. For the sake of discussion, we also assume that node j is constantly monitoring. Hence, if we consider l subgames, in each of the subgame, \mathcal{C}_i is updated.

We denote a random variable $y = \mathcal{C}_i = c_0 + \hat{n}_F c_F - \hat{n}_A g_A$. Since the mixed strategy profile requires node i to choose *Attack* with probability p^* , \hat{n}_F and \hat{n}_A are binomially distributed as:

$$\Pr(\hat{n}_F = \hat{N}_F) = C_l^{\hat{N}_F} [(1 - p^*)(1 - p_e)]^{\hat{N}_F} [1 - (1 - p^*)(1 - p_e)]^{l - \hat{N}_F} \quad (27)$$

$$\Pr(\hat{n}_A = \hat{N}_A) = C_l^{\hat{N}_A} [p^*(1 - p_e)]^{\hat{N}_A} [1 - p^*(1 - p_e)]^{l - \hat{N}_A} \quad (28)$$

Since $y = c_0 + \hat{n}_F c_F - \hat{n}_A g_A = c_0 + \hat{n}_F c_F - (l - \hat{n}_F)g_A = (c_F + g_A)\hat{n}_F - l g_A + c_0$ and l, c_F, g_A, c_0 are constants, to get the distribution of y , we first get the distribution of $w = y + l g_A - c_0$.

We use the probability generation function (pgf). For discrete random variable x , its pgf is defined as

$$G_X(z) = E[z^X] = \sum_{x=0}^{\infty} z^x \Pr(X = x) \quad (29)$$

The pgf for y is

$$\begin{aligned} G_W(z) &= E[z^W] = E[z^{\hat{N}_F(c_F + g_A)}] \\ &= \left\{ \sum_{\hat{n}_f=0}^l z^n C_l^{\hat{n}_f} [(1 - p^*)(1 - p_e)]^{\hat{n}_f} [1 - (1 - p^*)(1 - p_e)]^{l - \hat{n}_f} \right\}^{(c_F + g_A)} \\ &= \{(1 - p^*)(1 - p_e) + [1 - (1 - p^*)(1 - p_e)]z\}^{(c_F + g_A)l} \end{aligned} \quad (30)$$

Let $f^{(n)}(x) = \frac{\partial^n f(x)}{\partial x^n}$,

$$\mathbf{P}(w = k) = \frac{G_W^{(k)}(0)}{k!} \quad (31)$$

$$p^* = \frac{c_M}{[g_A(1 - p_e + \gamma p_e) - c_M] \Pr(\mathcal{C}_i \geq \tau) + (g_A - c_M)(1 - p_e) \Pr(\mathcal{C}_i < \tau) + c_M + \gamma g_A}. \quad (23)$$

$$q^* = \frac{c_A - g_A \gamma - c_F}{-(g_A + c_A)(1 - p_e) \Pr(\mathcal{C}_i < \tau) + (g_A \gamma - c_A)(1 - p_e)(\Pr(\mathcal{C}_i \geq \tau) - 1)} \quad (26)$$

The probability terms in (23) and (26) are given by,

$$\begin{aligned} \Pr(\mathcal{C}_i \geq \tau) &= \Pr(w \geq l g_A + \tau - c_0) \\ &= \sum_{n \geq l g_A + \tau} \frac{G_W^{(n)}(0)}{n!} \end{aligned} \quad (32)$$

$$\Pr(\mathcal{C}_i < \tau) = 1 - \sum_{n \geq l g_A + \tau - c_0} \frac{G_W^{(n)}(0)}{n!} \quad (33)$$

To relax the assumption of node j 's constant monitoring, the current stage t for the analysis is $[t = l/q^*]$. Therefore, we have obtained the equilibrium strategy parameter p^* and q^* for every subgame.

So far, we have shown that for the mixed strategy profile, attaining a Nash Equilibrium is feasible. As a matter of fact, every game has a mixed strategy Nash Equilibrium. To further refine the equilibrium, we apply the One-Shot Deviation Property to derive the condition for subgame perfect Nash Equilibrium. The property states:

DEFINITION 2: One-Shot Deviation Property (OSDP) [17]: No player can increase her payoff by changing her action at the start of any subgame in which she is the first-mover, given the other player's strategies and the rest of her own strategy.

We take node j as an example and assume the repeated game has no discount. In our previous equilibrium analysis using the indifference condition, we have proved that deviation from p^* or q^* will not increase the payoffs. Hence, in the following derivation, we show the deviation strategy is related to \mathcal{C}_i .

From (21) and (22), we can express the expected payoff for node j as:

$$\begin{aligned} U_j &= \sum_{t=0}^T q^* \{ [g_A(1 - p_e + \gamma p_e) - c_M] p^* \Pr(\mathcal{C}_i \geq \tau) \\ &\quad + (g_A - c_M) p^* (1 - p_e) \Pr(\mathcal{C}_i < \tau) \\ &\quad - (1 - p^*) c_M \} - (1 - q^*) p^* \gamma g_A. \end{aligned} \quad (34)$$

Suppose node j deviates at r th stage and $r \leq T$. The deviation can be either of the following two cases.

Case 1: Isolate node i while $\mathcal{C}_i \geq \tau$. In this case, if node j attacks and is successfully observed, it will be isolated. The expected payoff at this stage for node j is

$$\begin{aligned} U_{j,dev,1}^{(r)} &= \{ q^* \{ p^* (1 - p_e) (g_A - c_M) - p^* \gamma p_e (g_A + c_M) \\ &\quad - [p^* (1 - \gamma) p_e + (1 - p^*)] c_M \} \\ &\quad - (1 - q^*) p^* \gamma g_A \} \Pr(\mathcal{C}_i \geq \tau) \end{aligned} \quad (35)$$

Case 2: Keep node i while $\mathcal{C}_i < \tau$. Since node j only deviates one stage, node i will be isolated in the next stage.

The expected payoff for node j at this stage is the same as above expect for the last probability term.

$$\begin{aligned} U_{j,dev,2}^{(r)} &= \{ q^* \{ p^* (1 - p_e) (g_A - c_M) - p^* \gamma p_e (g_A + c_M) \\ &\quad - [p^* (1 - \gamma) p_e + (1 - p^*)] c_M \} \\ &\quad - (1 - q^*) p^* \gamma g_A \} \Pr(\mathcal{C}_i < \tau) \end{aligned} \quad (36)$$

In this way, the total expected payoff for node j under deviation is

$$U_{j,dev} = \sum_{t=0}^{r-1} U_j^{(t)} + U_{j,dev,1}^{(r)} + U_{j,dev,2}^{(r)} + \sum_{t=r+1}^T U_j^{(t)} \quad (37)$$

OSDP require $U_{j,dev} \leq U_j$. After algebraic manipulation, we have

$$\begin{aligned} g_A \gamma (q^* p_e + 1) + q^* p_e (\gamma c_M + 1 - \gamma) &\geq (1 - q^*) \gamma g_A \\ + q^* [\gamma g_A \Pr(\mathcal{C}_i < \tau) + p_e c_M \Pr(\mathcal{C}_i \geq \tau)] \end{aligned} \quad (38)$$

or

$$g_A \gamma [p_e + 1 - \Pr(\mathcal{C}_i < \tau)] \geq p_e [c_M \Pr(\mathcal{C}_i \geq \tau) + \gamma - 1 - \gamma c_M]. \quad (39)$$

To sum up, for the equilibrium on the post-detection game, we state the following theorem.

THEOREM 2: The post-detection game has a mixed strategy Nash Equilibrium when node i attacks with p^* and node j monitors with q^* . This strategy is also subgame perfect if $g_A \gamma [p_e + 1 - \Pr(\mathcal{C}_i < \tau)] \geq p_e [c_M \Pr(\mathcal{C}_i \geq \tau) + \gamma - 1 - \gamma c_M]$.

C. Convergence of the coexistence equilibrium

The post-detection game described above ends when $\mathcal{C}_i < \tau$. Since $\Pr(\mathcal{C}_i < \tau) > 0$, the game is of finite stages. In this subsection, we try to derive the expected length (number of stages) of the game.

We focus on the random variable \mathcal{C}_i . As we mentioned earlier, $\mathcal{C}_i = c_0 + \hat{n}_F c_F - \hat{n}_A g_A$. Again, we assume node j is constantly monitoring. After one stage game, the probability of $\hat{n}_F = \hat{n}_F + 1$ is $(1 - p^*)(1 - p_e)$, and the probability of $\hat{n}_A = \hat{n}_A + 1$ is $p^*(1 - p_e)$. Thus, we model the evolution of \mathcal{C}_i as a random process similar to a 1-dimensional random walk, where the value of \mathcal{C}_i increases by c_F with probability $(1 - p^*)(1 - p_e)$, and decreases by g_A with probability $p^*(1 - p_e)$. The $1 - p_e$ term comes from the unreliability of the channel. To obtain the expected length of the post-detection game, it is equivalent to calculating the expected first hitting time of the random process with the absorbing boundary $\mathcal{C}_i = \tau$.

THEOREM 3: The expected length of the post-detection game is

$$\sum_{\eta > 0} \eta \frac{\binom{\eta}{\hat{n}_F} - \sum_d \hat{n}_F^{-1} \binom{(c_0 - \tau)/c_F + d}{\frac{g_A/c_F}{d} + d} (\eta - \frac{(c_0 - \tau)/c_F + d}{\frac{g_A/c_F}{\hat{n}_F - d} - d})}{2^\eta}.$$

Proof: Let η be a random variable representing the first hitting time. We assume that time is divided into slots and each slot represent a stage game. It is easy to see that $\eta = \hat{n}_F + \hat{n}_A$. At every slot, the random process has 2 possible evolution directions, i.e., $\hat{n}_F + 1$ or $\hat{n}_A + 1$. Therefore, for η slots, there are 2^η possible realizations.

We try to calculate how many paths hit the boundary exactly on the η th slot. The following notations are made. Let $m = \frac{g_A}{c_F}$, $s = (c_0 - \tau)/c_F$ and m, s are integers. In Figure 2, we interpret how to move on a grid according to a random process. Consider a random walk from the left bottom point. If \hat{n}_F increases, move one block right. If \hat{n}_A increases, move m blocks up. While each block is a squarelet with the length c_F , the width of the grid is $\hat{n}_F c_F$, the height is $g_A \hat{n}_A$, and diagonal line represents $C_i = \tau$. Each walk consists of η moves and must end on or beyond the upper rightmost corner. What we are interested in is the number of monotonic paths that wholly falls under the diagonal line, because each of those paths is a realization of the random process which hits the boundary for the first time at the η th slot.

While counting the number of realizations under the diagonal line might be difficult, we calculate the realizations that do cross the line. Let the number of realizations crossing the line be M , the number of realizations under the line is then $C_n^{\hat{n}_F} - M$, where $C_n^{\hat{n}_F}$ is the total number of possible realizations on the grid. Consider a sample realization crossing the line as shown in Figure 2. Let d be the number of horizontal steps taken in the path before hitting the diagonal line. To hit the line, at least $\frac{s+d}{m}$ vertical steps should be taken, covering a total height of $(d+s)c_F$. The total number of such paths is $\sum_d C_{\frac{s+d}{m}+d}^d$. After hitting the line, the rest of the path should consist of $\hat{n}_F - d$ vertical steps and the total number of moves left is $\eta - \frac{s+d}{m} - d$. So, the total number of paths that cross the diagonal line is $M = \sum_d^{\hat{n}_F-1} C_{\frac{s+d}{m}+d}^d C_{\eta - \frac{s+d}{m} - d}^{\hat{n}_F - d}$.

To sum up, out of 2^η realizations, $C_n^{\hat{n}_F} - \sum_d^{\hat{n}_F-1} C_{\frac{s+d}{m}+d}^d C_{\eta - \frac{s+d}{m} - d}^{\hat{n}_F - d}$ realizations hit the diagonal line for the first time at the η th move. The probability of game length being η is then $\frac{C_n^{\hat{n}_F} - \sum_d^{\hat{n}_F-1} C_{\frac{s+d}{m}+d}^d C_{\eta - \frac{s+d}{m} - d}^{\hat{n}_F - d}}{2^\eta}$. Finally, we can express the expected length of the post detection game as

$$E[length] = \sum_{\eta>0} \eta \frac{C_n^{\hat{n}_F} - \sum_d^{\hat{n}_F-1} \binom{\frac{s+d}{m}+d}{d} \binom{\eta - \frac{s+d}{m} - d}{\hat{n}_F - d}}{2^\eta}. \quad (40)$$

IV. SIMULATIONS

In this section, we study the properties of the perfect Bayesian Nash equilibrium in the malicious node detection game and the post-detection subgame perfect Nash equilibrium through simulations. In our simulator, two players play the games repeatedly; the payoffs and strategy profiles for each of the subgames are recorded to analyze the properties of the equilibria.

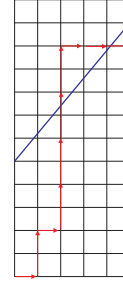


Fig. 2. Realizations of the random walk.

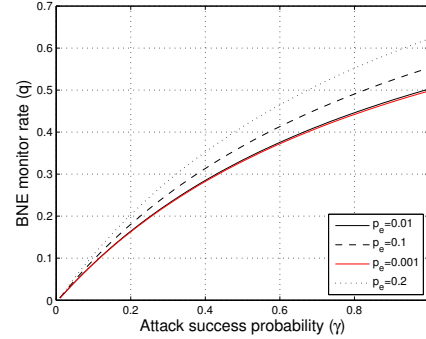


Fig. 3. Equilibrium strategy q vs. the attack success rate in malicious node detection game.

A. Malicious node detection game

We first present the simulation results on the malicious node detection game. In Figure 3, we show how the monitoring probability in PBE strategy increases with the malicious node attack success rate. The plots infer that the equilibrium require node j to increase its monitoring frequency as the attack success rate increases. Also, as the channel becomes more unreliable, node j must play *Monitor* more frequently..

Figure 4 compares the convergence of node j 's belief system when different attack gains are presented. The plots are shown with $p_e = 0.01$, $\gamma = 0.95$ and $\alpha = 0.01$. In Figure 4(a), we show how the belief system forms a correct belief on the type of node i when only *Attack* is observed. The convergence of the belief system under PBE is illustrated in Figure 4(b). The plots suggest that the lower the attack gain is, the quicker the belief system converges. This property can be explained as follows. A smaller attack gain requires node i to attack more often in order to get more payoff, and increasing the attack frequency also increases the risk of being successfully observed. With more observations, the belief is updated more frequently and accurately. Belief system converges slower in Figure 4(b) than in Figure 4(a) because in the PBE, instead of constantly monitoring, node j only monitors with probability q .

A more complete study on the convergence of the belief system is shown in Figure 5. Plots in Figure 5(a) indicate the larger the disguise cost c_F/c_A is, the less time it takes to converge. This is because, with a larger disguise cost, it is unprofitable for node i to disguise by forwarding packets. Instead, it will launch more attacks, thus increasing the chances to be identified. Figure 5(b) shows a quicker converged belief

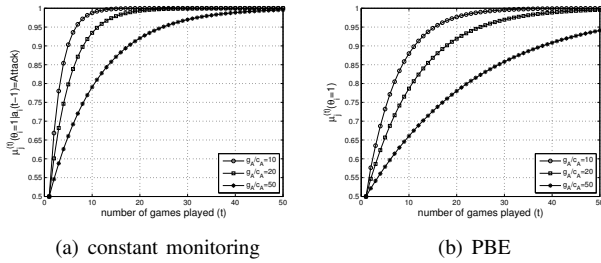


Fig. 4. Belief system update with different attack gains.

system for a smaller detection gain. Figures 5(c) and 5(d) relate the convergence with less errors and uncertainties in the system. As expected, with errors and uncertainties (i.e., low channel loss, high attack success rate and low false alarm rate), the belief system converges quickly.

Finally, the parameters affecting the PBE attack probability p are investigated in Figure 6. The attack gain is a very important factor in determining the value of p as shown in Figure 6(a). A large attack gain means more payoff gained from an attack, which implies less number of attacks are needed. Hence p should be smaller. Figures 6(b) and 6(c) indicate that node i should attack less frequently under a reliable channel as every attack is more likely to be successful. However, as suggested in Figure 5(d), if the false alarm rate is high for the regular node, the malicious node can take advantage of it and attack more often.

B. Post-detection game

After the belief system of node j converges ($\theta_i \geq 0.99$), we can safely conclude that node j has detected the malicious node. Therefore, the post-detection game starts. To show the continuity, at the beginning of the post detection game, node i sticks to its PBE strategy.

Figure 7 presents how the strategy profile p^* evolves to the SPNE strategy from the PBE. It is clear in the plots that in the SPNE, node i should decrease its attack probability to avoid isolation. Figure 7(a) shows a larger detection gain that corresponds to a smaller attack rate; thus in the equilibrium, the payoffs for node j will not increase due to the large detection gain. Figure 7(b) states that if the channel is lossy, node i should attack more often. The reason behind this claim is that the more unreliable the channel is, the less probable node j can accurately observe an attack. Plots in Figure 7(c) are obtained from detection gain equals to 5. This figure shows that the equilibrium is not sensitive to the initial value and threshold of the coexistence index \mathcal{C}_i .

The expected length of the post-detection game is shown in Figure 8. First, the figure states that the less errors (i.e., less channel loss and more successful attack) in the system, the longer the post-detection games can be played. Second, the length of the game grows with the attack gain. This interesting phenomena can be explained in the following way. The larger attack gain enables the malicious node to attack less while keeping its payoff high. Thus, more often, the malicious node will play as a regular node to avoid isolation. This will increase the time for the regular and

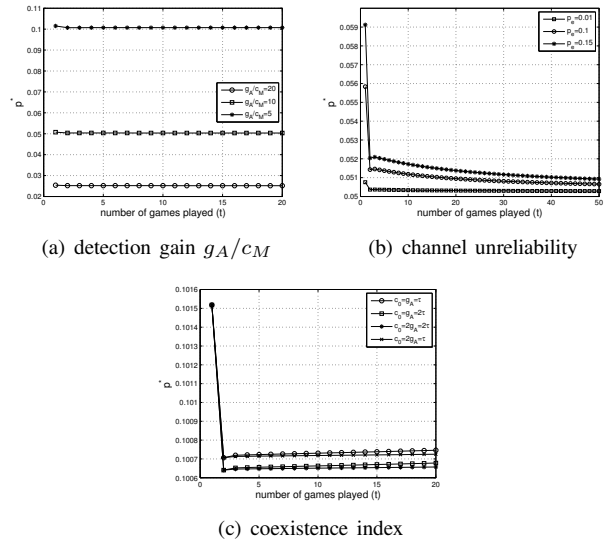


Fig. 7. Effects of parameters on the SPNE strategy p^* .

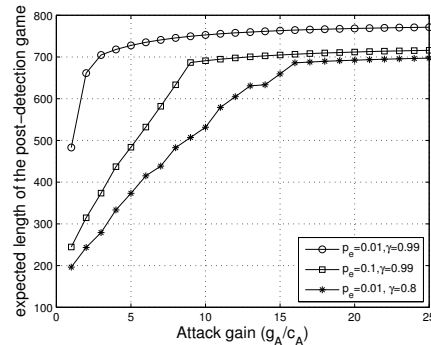


Fig. 8. Expected length of the post-detection game.

malicious nodes to coexist. This property can be used to extend the lifetime of the network.

Last but not the least, we show how the network throughput can benefit from coexistence. Similar observations can be made as the game length property. With a larger attack gain, the malicious node decreases its attack rate and does more packet forwarding as a regular node. Therefore, the malicious nodes can be utilized to increase the throughput more often as the attack gain grows. The throughput gain property illustrates clearly that malicious and regular nodes can coexist, and the coexistence equilibria improve the throughput of the network.

V. CONCLUSIONS

In this paper, we apply game theory to study coexistence of malicious and regular nodes in a wireless network with unreliable channels. We formulate a malicious node detection game and a post-detection game played by the regular and malicious nodes. While both games are of imperfect information type, we show that the former game has a mixed strategy perfect Bayesian Nash equilibrium and provide a solution to achieve that equilibrium. For the latter game, a coexistence index is proposed. We also prove that while keeping the coexistence index above a threshold, the post-detection game has a subgame perfect Nash Equilibrium

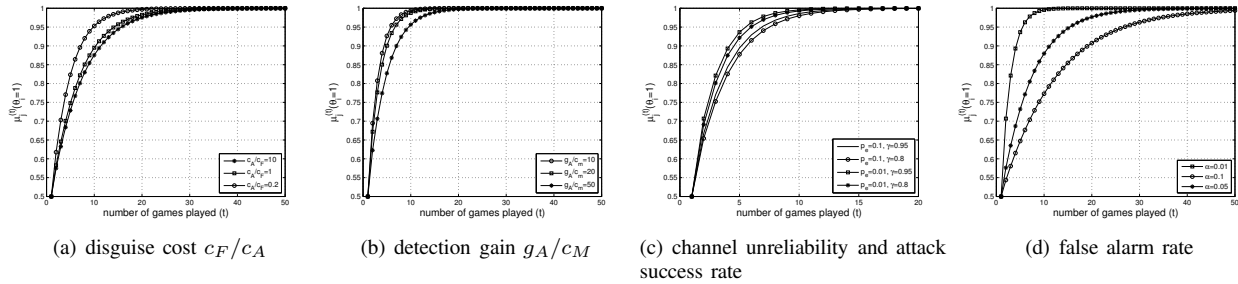


Fig. 5. Effects of parameters on belief system update.

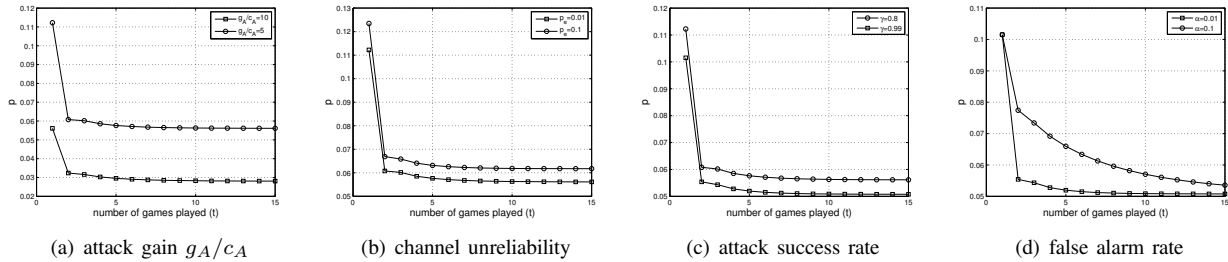


Fig. 6. Effects of parameters on the PBE strategy p .

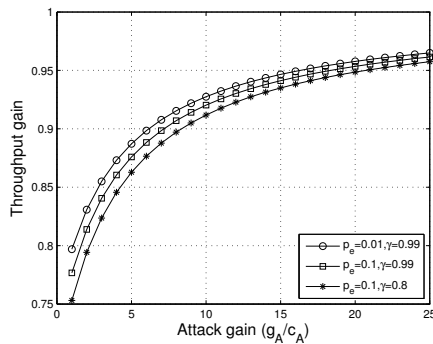


Fig. 9. Throughput gain.

which is also the coexistence equilibrium for malicious and regular nodes. Simulations are provided to illustrate the properties of the equilibria. In particular, we show how the system parameters like attack gain, attack success rate, detection gain and channel loss affect the convergence of the games and the equilibrium strategies. Simulation results also state that the coexistence equilibrium helps to extend the length of the games and improves the throughput of the network.

REFERENCES

- [1] A. Agah, S. K. Das, K. Basu and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach", *IEEE NCA 2004*, pp. 343-346.
- [2] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents", *ACM Mobicom 2003*, pp. 245-259.
- [3] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad-hoc networks", *ACM/Kluwer Mobile Networks and Applications*, 8(5), pp. 579-592.
- [4] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks", *Performance Evaluation*, 57(4), pp. 427-439.
- [5] D. Fudenberg and J. Tirole, *Game Theory*, MIT press, Cambridge, MA, 1991.

- [6] J. J. Jaramillo and R. Srikant, "DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks", *ACM MobiCom 2007*, pp. 87-97.
- [7] Z. Ji, W. Yu and K. J. R. Liu, "Cooperation enforcement in autonomous MANETs under noise and imperfect observation", *IEEE Secon 2006*, pp. 460-468.
- [8] M. Kodialam and T. V. Lakshman, "Detecting network intrusion via sampling: a game theoretic approach", *IEEE INFOCOM 2003*, pp. 1880-1889.
- [9] D. M. Kreps and R. Wilson, "Sequential Equilibria", *Econometrica* 50(4), pp.863-894, 1982.
- [10] F. Li and J. Wu, "Hit and Run: A Bayesian Game Between Malicious and Regular Nodes in MANETs", *IEEE SECON 2008*, pp. 432-440.
- [11] X.-Y. Li, Y. Wu, P. Xu, G. Chen and M. Li, "Hidden Information and Actions in Multi-Hop Wireless Ad Hoc Networks", *ACM Mobihoc 2008*, pp. 283-292.
- [12] P. Liu, W. Zhang and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", *ACM Trans. on Information and System Security*, 56(3), pp. 78-118, 2005.
- [13] Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks", *ACM GameNets 2006*.
- [14] A. B. Mackenzie and L. A. DaSilva, *Game Theory for Wireless Engineers*, San Rafael, California: Morgan & Claypool Publishers, 2006.
- [15] P. Michiardi and R. Molva, "Analysis of coalition formation and cooperation strategies in mobile ad hoc networks", *Ad Hoc Networks*, 3(2005), pp. 193-219.
- [16] F. Milan, J. J. Jaramillo and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes", *ACM GameNets 2006*.
- [17] M. J. Osborne, "An introduction to Game Theory", *Oxford University Press*, New York, NY, 2004.
- [18] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks", *Proceedings of IEEE Infocom 2003*, pp. 807-817.
- [19] G. Theodorakopoulos and J. S. Baras, "Malicious Users in Unstructured Networks", *IEEE INFOCOM 2007*, pp. 884-891.
- [20] W. Wang, S. Eidenbez, Y. Wang and X.-Y. Li, "OURS: Optimal unicast routing system in non-cooperative wireless networks", *ACM Mobicom 2006*, pp. 402-413.
- [21] S. Zhong, L. Li, Y. Liu and Y. Yang, "On Designing Incentive-Compatible Routing and Forwarding Protocols in Wireless Ad-Hoc Networks—An Integrated Approach Using Game Theoretical and Cryptographic Techniques", *ACM Mobicom 2005*, pp. 117-131.