Attack and Flee: Game-Theory-Based Analysis on Interactions Among Nodes in MANETs

Feng Li, *Member, IEEE*, Yinying Yang, *Student Member, IEEE*, and Jie Wu, *Fellow, IEEE*

***Abstract*—In mobile ad hoc networks, nodes have the inherent ability to move. Aside from conducting attacks to maximize their utility and cooperating with regular nodes to deceive them, malicious nodes get better payoffs with the ability to move. In this paper, we propose a game theoretic framework to analyze the strategy profiles for regular and malicious nodes. We model the situation as a dynamic Bayesian signaling game and analyze and present the underlining connection between nodes' best combination of actions and the cost and gain of the individual strategy. Regular nodes consistently update their beliefs based on the opponents' behavior, while malicious nodes evaluate their risk of being caught to decide when to flee. Some possible countermeasures for regular nodes that can impact malicious nodes' decisions are presented as well. An extensive analysis and simulation study shows that the proposed equilibrium strategy profile outperforms other pure or mixed strategies and proves the importance of restricting malicious nodes' advantages brought by the flee option.**

***Index Terms*—Bayesian signaling game, game theory, mobile ad hoc networks (MANETs), mobility, reputation systems, sequential rationality, uncertainty.**

I. Introduction

THE COLLABORATION between the participants is the foundation for mobile ad hoc networks (MANETs) to achieve the desired functionalities. The topologies in MANETs change dynamically because of node movement. Nodes in MANETs usually have no predefined trust between each other. Moreover, all nodes tend to maximize their own *utility* (also referred to as *payoff*) in activities. Among existing research, different mechanisms (e.g., reputation systems, virtual currency, and barter economy) have been developed to stimulate cooperation and mitigate nodes' selfish behavior.

Aside from regular nodes' selfish behavior, malicious nodes also exist in the network. The common objective of malicious nodes is maximizing the damage to the network while avoiding being caught. Their utility comes from activities that disrupt the operation of the network and waste the resources of regular nodes.

Manuscript received January 5, 2009. First published December 22, 2009; current version published June 16, 2010. This work was supported in part by NSF grants CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240. This paper was recommended by Associate Editor T. Vasilakos.

F. Li is with the School of Engineering and Technology, Indiana University-Purdue University Indianapolis, Indianapolis, IN 46022 USA (e-mail: fengli@iupui.edu).

Y. Yang is with the Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, FL 33431 USA.

J. Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122 USA (e-mail: jiewu@temple.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMCB.2009.2035929

In order to minimize the impact of malicious nodes and stimulate cooperation, regular nodes monitor and continuously evaluate their neighbors. Certain criteria are set to distinguish a node's trust level toward others. Regular nodes will focus their resources on cooperating with neighbors that they trust, decline requests from suspicious neighbors, and report when a neighbor is considered to be malicious. However, in this case, intelligent malicious nodes would elaborately choose a frequency at which they cooperate to deceive regular nodes.

Moreover, malicious nodes have the strategy of fleeing to avoid punishment in MANETs. Therefore, a malicious node can start its malicious behavior all over again with a clean history in a new location by fleeing before being caught. However, this additional strategy does not imply that malicious nodes should continuously attack and run since fleeing is also associated with a cost (e.g., the energy spent to move to the selected destination). We can instinctively describe the malicious nodes' optimal strategy as follows: cooperate to deceive regular nodes' trust, attack to cause damage and maximize their own utility, and flee before regular nodes accumulate enough evidence and decide to report. Now, we need to answer some critical questions in MANETs: How will a node choose its strategy according to its type? When should a regular node report? When should a malicious node flee? What countermeasures are available to restrict the malicious node's advantages brought by the flee strategy?

We model the wrestling between the regular and malicious node as a *dynamic Bayesian game* and provide answers to the aforementioned questions through analysis. In this game, nodes observe the result of each round of communication. Each node's type, regular or malicious, is its own private information. Its neighbor's actual type is the incomplete information in the game. Each node should form beliefs toward neighbors and update the beliefs according to the neighbors' actions as the game evolves.

Both regular and malicious nodes' best responses are guided by threats about certain reactions from other players. Such threats are dependent on their current beliefs. The regular node sets a reputation threshold and judges other nodes' types based on the evaluated belief and this threshold. The malicious node continuously evaluates the risk, which is decided by the possibility that a regular node would choose to report under current conditions. On the basis of the risk and expected fleeing cost, the malicious node makes a decision on fleeing.

The contributions of this paper are as follows: 1) We formulate a Bayesian game framework to study the strategy of regular and malicious nodes in MANETs; 2) we propose decision rules for regular nodes to report and malicious nodes to flee, which

comply with the sequential rationality requirement; 3) we study the equilibrium strategy profiles for both parties based on the belief and expected payoff and reveal the connection between nodes' best response and the cost and gain of each individual strategy; and 4) we present several countermeasures to restrict the flee strategy.

II. Related Work

The incentives for nodes to cooperate are analyzed and presented in [1]–[3]. However, in these works, malicious nodes are modeled as never cooperative, without any further sophistication, since their main focus was discouraging selfish nodes. There is no degree of selfishness that can approximate the behavior of malicious nodes. In this paper, we model the malicious nodes with their own utility functions, which are different from regular nodes. In other words, we assume that malicious nodes are also rational concerning their goals.

Some recent works have studied the incentives for malicious nodes and modeled their behavior more rationally. In [4], Liu *et al.* present a general incentive-based method to model the attackers' intents, objectives, and strategies. In [5], Theodorakopoulos and Baras further study the payoff of the malicious nodes and identify the influence of the network topology. However, the good nodes' behavior in [5] is simple, and it fails to consider the possibility that an attacker might choose different attack frequencies toward different opponents. We consider more "intelligent" malicious nodes, making the regular and malicious nodes' game in this paper more realistic.

Game theory [6] is a powerful tool in modeling interactions among self-interested nodes and predicting their choice of strategies [7]–[10]. Therefore, wireless ad hoc networks [11]–[13] are often studied using game theory. The equilibria of the contention window game are studied in [13]. The results of the analysis show that selfishness does not always lead to network collapse and may help the network to operate at an efficient Nash equilibrium. In [11], a mixed-strategy equilibrium is studied to counter the jamming attack. A Bayesian game is studied in [12] to save energy in distributed intrusion detection systems. In this paper, we utilize game theory [6] to analyze the typical wrestling scenario between regular and malicious nodes in MANETs.

We use a monitoring and reputation system [14]–[17] as the basic setting for regular nodes. Many related works also use reputation systems [18]–[20] and a game theory model [21] to analyze the problem. Srinivasan *et al.* [22] analyze a modified tit-for-tat strategy, where each node compares its own frequency to the aggregate frequency of cooperation of the network. Altman *et al.* [23] propose a scheme for punishing users whose frequency of cooperation is below the level dictated by the Nash equilibrium.

III. Basic Model and Assumptions

Table I lists the notations used in this paper. We consider a MANET which contains both regular and malicious nodes. We will not restrict malicious nodes' ability to coordinate. Hence, they would avoid playing the following game with each other because there is no gain in doing so. Regular nodes only know their own type. To simplify the analysis, time is divided into slots, and players choose their strategies simultaneously at the beginning of each time slot. A sample scenario for the regular and malicious nodes game is shown in Fig. 1(a).

TABLE I
Notations and Acronyms

$A/C/D$	Attack/Cooperate/Decline.
F/R	Flee/Report.
$C_A/C_C/C_F/C_R$	Cost for attack/cooperate/flee/report.
$G_A/G_C/G_R$	Gain for attack/cooperate/report.
L_F	Loss for false alarm.
α	The number of detected cooperations.
β	The number of detected attacks or declines.
$u/b/d$	Uncertainty/Belief/Disbelief in the opinion.
θ	The probability that a node is a malicious node.
ϕ	The probability that a malicious node attacks.
p	The probability that a regular node cooperates.
σ/σ^*	Strategy profile/Equilibrium strategy profile.
T	Uncertainty threshold.
$E(\cdot)/VAR(\cdot)$	Expected value/variance.
BNE/PNE	Bayesian Nash/Perfect Bayesian Equilibrium.

As shown in Fig. 1(b), the regular user can choose to cooperate or decline one round of communication, while the malicious node can attack or cooperate. Here, *decline* (D) means that a node simply rejects participation, while *cooperate* (C) means that a node makes itself available for communication. The packet can be forwarded through a link only when nodes on both endpoints of the link choose to cooperate. The regular node benefits from good network operations. However, each receiving and forwarding action also costs energy. If a regular node chooses to cooperate while the other node on the link chooses not to, the regular node wastes energy.

The malicious node *attacks* (A) in an effort to waste the resources and disrupt the operation of the network. Attacking leads to a failure of one round of communication between two neighbors. Malicious nodes can conduct a simple dropping-packet attack, which is in the same form as the decline strategy of regular nodes. However, malicious nodes get payoff from the attack, while regular nodes receive no gain from the decline. Malicious nodes can also conduct more sophisticated attacks, such as analyzing a received packet without further forwarding or sending out a modified packet. To make the definition of "attack" more general, we use the cost and gain metrics to summarize the characteristic of one type of attack in the game. Different attack mechanisms have different costs and expected gains; however, the game-based analysis framework is equally applicable to these attacks.

Neighbor Monitoring: By exploiting the promiscuous nature of broadcast communication in wireless media, nodes track the outgoing packets of their one-hop neighbors through passive observation. However, a node cannot distinguish whether a failure in communication is caused by its opponent's A or D (A/D for short). Therefore, an observation is classified as either a detected C or a detected A/D. Accordingly, the corresponding discrete variable, namely, α for detected C and β for detected A/D, is incremented as shown in Fig. 1(b). This mechanism is called *neighbor monitoring* [24].

In practical MANETs, the detection process has challenges. First, the malicious node can disguise itself. Second, the

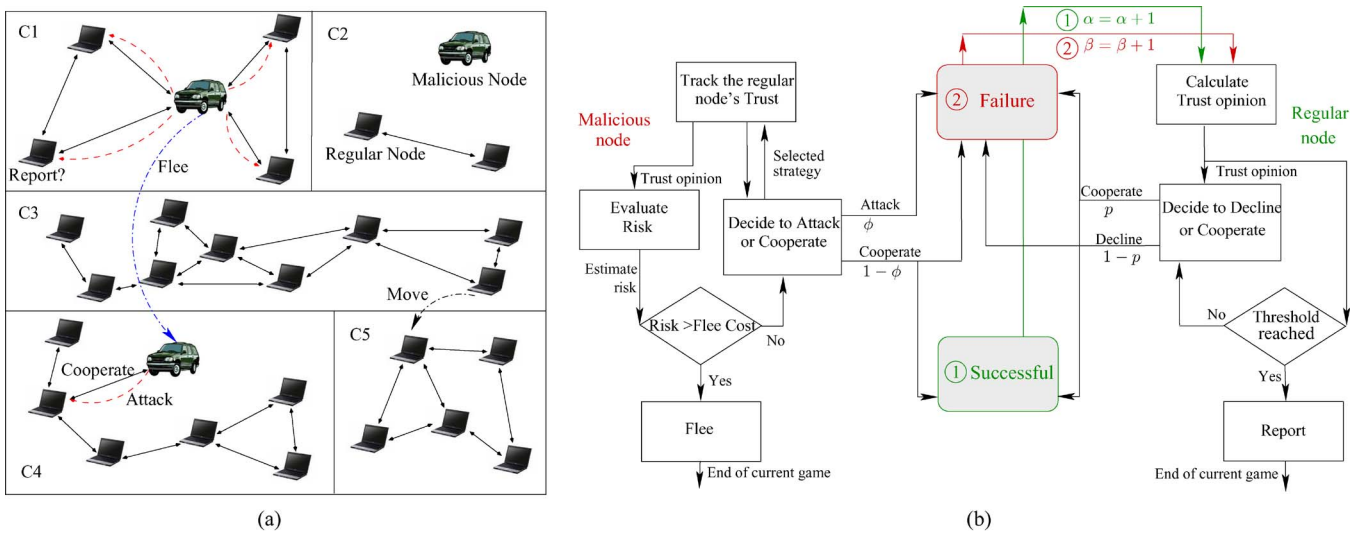


Fig. 1. Wrestling between regular and malicious nodes in MANETs. (a) Example scenario. (b) Decision process.

randomness and unreliability of the wireless channel bring more uncertainty to the monitoring process. A scheme which ignores the noise in the observation is not practical in the actual wireless networks. We assume that the error in observation may occur but with very low probability. Otherwise, it would be impossible to distinguish a malicious node by neighbor monitoring.

Cluster: A *cluster* denotes a logical region of a MANET where nodes are highly connected with each other. The grid in Fig. 1 indicates a cluster. A MANET can always be divided into clusters. Nodes can dynamically leave or join a cluster during their movement. We assume that an authentication method exists and that the identity is bounded with the physical node which cannot be changed or faked during the node's stay in the cluster. When a node first joins a cluster, other nodes in the cluster authenticate the node and set their belief toward the newcomer to the initial value.

When a malicious node *flees* (F) into a cluster that it has never visited before, nodes in that cluster will treat it as a newcomer. This is because a node's behavior cannot be tracked and the identity binding cannot be monitored outside the cluster. In essence, the flee strategy leads to a reputation reset. When a regular node decides to *report* (R) one of its neighbors as a malicious node, it broadcasts the report in its current cluster. If the report is considered to be true, the malicious node being reported will be punished. Otherwise, the reporting node's accountability will be affected for the false alarm.

Decision Process: Fig. 1(b) shows the general decision process of regular and malicious nodes. The regular node obtains feedback from the neighbor monitoring and evaluates the belief and sufficiency of evidence toward the opponent based on α and β. It follows a threshold policy to decide whether to report. If not, the regular node chooses C with a probability p, which is calculated based on its belief. The malicious node also evaluates the risk of being caught. It follows its rule to decide whether to flee. If not, the malicious node chooses A with a probability ϕ. The key issues in this decision process are the decision rules for both parties and the action profiles reflected by p and ϕ. We analyze the MANET to find the optimal decision rules and action profiles by using the dynamic Bayesian game framework.

Bayesian Signaling Game: The regular/malicious node game in this paper is a multistage dynamic Bayesian signaling game. *Bayesian games* are the combination of game theory and probability theory that allow taking incomplete information into account. In Bayesian games, each player is allowed to have some private information that affects the progress of the game. Others are assumed to have beliefs about the private information. Players choose their actions during the game according to their beliefs and private information. *Signaling games* are one specific category of Bayesian games. There are two kinds of players in signaling games: senders and receivers. The sender's type is its private information. Based on its own type, the sender chooses to send a message from a set of possible messages. The receiver observes the message but not the type of sender.

Stage games are simple games played at individual time slots. The objective of both regular and malicious nodes is to maximize their expected payoff, which implies that both players are *rational*. The Nash equilibrium for a single stage game given nodes' current beliefs is called *Bayesian Nash equilibrium* (BNE). For a multistage game, the notion of *sequential rationality* means that a player's strategy should be the best response to others' strategies according to its prediction, and it is what determines the optimality of the subsequent play.

Through analysis, we aim to find the *perfect Bayesian equilibrium* (PBE) of this game. PBE is a refinement of BNE. PBE requires that players form beliefs about the opponents' types, update the beliefs, and take the best response actions using these beliefs.

IV. Regular/Malicious Node Game

We model the regular/malicious node game as a multistage dynamic Bayesian signaling game to find the optimal strategy of regular and malicious nodes.

TABLE II
STRATEGIC FORM OF THE REGULAR/MALICIOUS NODE GAME.
(a) NODE i IS MALICIOUS: (i'S UTILITY, j'S UTILITY).
(b) NODE i IS REGULAR: (i'S UTILITY, j'S UTILITY)

(a)

	C	D	R
A	$(G_A - C_A, -G_A - C_C)$	$(-C_A, 0)$	$(-G_R - C_A, G_R - C_R)$
C	$(-C_C, G_C - C_C)$	$(-C_C, 0)$	$(-G_R - C_C, G_R - C_R)$
F	$(-C_F, -C_C)$	$(-C_F, 0)$	$(-C_F, -C_R)$

(b)

	C	D	R
C	$(G_C - C_C$, same)	$(-C_C, 0)$	$(-C_C, -L_F - C_R)$
D	$(0, -C_C)$	(0, 0)	$(0, -L_F - C_R)$
R	$(-L_F - C_R, -C_C)$	$(-L_F - C_R, 0)$	$(-L_F - C_R$, same)

A. Game Specification

In the game, player i is the sender, and its type can be regular or malicious; player j is a regular node, and it is the receiver. In each time slot, each player chooses its action from its strategy space. The strategy space for regular nodes is $\{C, D, R\}$. For malicious nodes, the strategy space is $\{A, C, F\}$. After each time slot, each player receives a payoff that depends on its own action, its neighbors' actions, and its own type. The payoffs are listed in Table II.

For both players, all possible strategies, except D, incur cost. The cost can be interpreted as the energy spent to conduct certain actions. For a malicious node, it gains G_A from a successful A. The success depends on its neighbor's strategy. Only when regular node j selects C will the attack succeed. The malicious node could also choose C to deceive node j; however, there is no gain for the malicious node if it chooses C in a one-shot game, as it has a different objective compared to regular nodes. Regular nodes gain G_C from a successful C. They could also choose D, which incurs zero gain and no cost even if the opponent chooses A in a stage game.

Both players have one more option. When choosing F, the malicious node avoids the risk of being caught. Therefore, the expected gain for F is the value of risk. This risk is not static; it increases as the regular node j's evidence accumulates. If j chooses R, it gets the gain G_R if i is a malicious node. The malicious node is considered to be caught in this case. However, j should also consider the possible loss for false alarm. If i is a regular node and j reports i as a malicious node, node j needs to bear the loss L_F for this false alarm.

B. Belief System

In the game, node j needs to update its belief according to the game evolution. We propose a certainty-oriented reputation system (CORS) for belief updating.

In the CORS, nodes use a neighbor monitoring mechanism. Each node estimates its neighbor's type based on its accumulated observations using the Bayesian inference, which is a statistical model to update the probability that a hypothesis is true according to the evidence. Beta distribution $Beta(\alpha, \beta)$ is used in the Bayesian inference. The beta distribution is a family of continuous probability distributions defined on [0, 1] differing in the values of their two non-negative shape parameters α and β. To start with, node j has the prior $Beta(1, 1)$ for node i. The prior $Beta(1, 1)$ implies the uniform distribution on [0, 1], which indicates complete uncertainty as there is no observation. When observation result $(\alpha - 1, \beta - 1)$ is obtained from neighbor monitoring, the prior is updated as $Beta(\alpha, \beta)$.

Many reputation systems use Bayesian inference to reason nodes' trust opinions. However, trust opinions are usually sharply divided into belief or disbelief in these systems. A simplistic belief update rule, which calculates b as $\alpha/(\alpha + \beta)$, is generally used. However, this omits the possible cost for false positive, which is important for regular nodes' sequential rationality. The main cause of false positive is the uncertainty in nodes' opinion.

We use a triplet to represent node j's (trustor) opinion toward another node i (trustee) in the CORS: $(b, d, u) \in [0, 1]^3$ and $b + d + u = 1$, where b, d, and u designate belief, disbelief, and uncertainty, respectively [18].

Two important attributes can be observed from the general understanding of the concept of uncertainty. First, when there is more evidence, u will consequently be lower. Second, when the evidence for detected C or A/D dominates, there will be less u when compared to the equal-evidence situation. After examining the major statistical metrics of the beta distribution, we find that the normalized variance satisfies these observations. Therefore, we define u as follows:

$$u = \frac{12 \cdot \alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)}. \tag{1}$$

The numerator and the denominator guarantee the latter and the former attributes, respectively. The total certainty is $(1 - u)$, which can be divided into b and d according to their share of supporting evidence. Hence, $b = (\alpha/(\alpha + \beta)) \cdot (1 - u)$, and $d = (1 - u) - b = (\beta/(\alpha + \beta)) \cdot (1 - u)$.

Assume that we have two cases: 1) $\alpha = \beta = 10$ and 2) $\alpha = \beta = 5$. Although $\alpha/(\alpha + \beta) = 0.5$ is the same in both cases, the uncertainty u is 0.14 in case 1) and 0.27 in case 2).

C. Stage Game

Both players are rational in the sense that the malicious node would like to follow strategies that minimize its chance of being caught and maximize the damage. The regular node also wants to play strategies that will maximize its chances of catching malicious nodes without losing the opportunity to cooperate with other regular nodes. The extensive form of the game is given in Fig. 2. Nature determines the type of node i, and this type is i's private information. Node j's current belief that i's type is malicious is represented by θ. Recall that α and β denote the number of detected C and detected A/D in the previous stage games, respectively. According to Bayes' rule, θ should be calculated as $\theta = \beta/(\alpha + \beta)$, while $1 - \theta = \alpha/(\alpha + \beta)$. We assign the initial value $\alpha = \beta = 1$ at the beginning, which makes $\theta = 0.5$. This initial belief is in compliance with the no-evidence situation.

We analyze the possible BNE. The Nash equilibrium refers to the situation where each player has chosen a strategy and no player can benefit by changing its strategy while the others maintain theirs. We discuss pure-strategy BNE under two cases. In the first case, node i plays its pure strategy

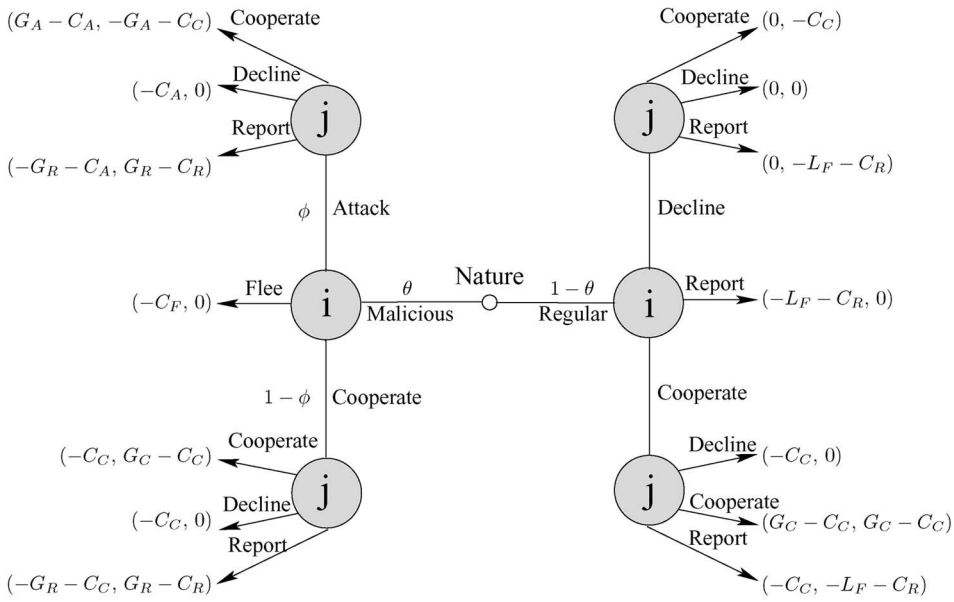


Fig. 2. Single stage of the flee game.

$\sigma_i = (A$ if malicious, C if regular), which means that i always plays A if its type is malicious and C if it is regular. The expected payoffs $E_j(C)$ or $E_j(D)$ of j playing its pure strategy $\sigma_j = C$ or $\sigma_j = D$ are

$$\begin{cases} E_j(C) = \theta \cdot (-G_A - C_C) + (1-\theta) \cdot (G_C - C_C) \\ E_j(D) = \theta \cdot 0 + (1-\theta) \cdot 0. \end{cases}$$

The formula of $E_j(C)$ enumerates two cases. One is that neighbor node i is a malicious node. According to j's current belief, this case appears with the probability θ. Since i will choose A, j's payoff in this case is $(-G_A - C_C)$. Another case is that i is a regular node, which appears with the probability $1-\theta$. j's payoff in this case is $(G_C - C_C)$. Other formulas in this section follow the same idea.

If $E_j(C) \geq E_j(D)$, node j's best response is to play C. That is, when the estimated probability $\theta \leq (G_C - C_C)/(G_C + G_A)$, the BNE strategy pair for i and j is $(\sigma_i, \sigma_j) = ((A$ if malicious, C if regular), $C)$. However, when $\theta > (G_C - C_C)/(G_C + G_A)$, there is no pure-strategy BNE because, when the malicious-type node i plays A, the best response for j is to play D. However, if j plays D, it is possible that C is the best response for malicious-type node i since C_A could be larger than C_C in some scenarios.

In the second case, malicious-type node i plays pure strategy C. Then, j's best response is C, regardless of θ. However, if j plays C, malicious-type node i's best response is A, which reduces to the previous case. In this case, $(\sigma_i, \sigma_j) = ((C$ if malicious, C if regular), $C)$ is not a BNE.

We now examine the mixed-strategy BNE for situations without a pure-strategy BNE. Recall that ϕ stands for the probability that the malicious-type node i will play A, and p stands for the probability that node j will play C. j's expected payoffs of C and D are

$$\begin{cases} E_j(C) = \phi \cdot \theta \cdot (-G_A - C_C) + (1 - \phi \cdot \theta) \cdot (G_C - C_C) \\ E_j(D) = \phi \cdot \theta \cdot 0 + (((1-\phi) \cdot \theta) + (1-\theta)) \cdot 0. \end{cases}$$

To make C and D indifferent to j, i.e., $E_j(C) = E_j(D)$, the malicious-type node i's equilibrium strategy is to play A with $\phi = (G_C - C_C)/((G_C + G_A) \cdot \theta)$. i's expected payoffs of A and C are

$$\begin{cases} E_i(A) = p \cdot G_A - C_A \\ E_i(C) = -C_C. \end{cases}$$

By imposing $E_i(A) = E_i(C)$ to make A and C indifferent to malicious-type node i, we get that j's equilibrium strategy is to play C with probability $p = (C_A - C_C)/G_A$ (when $C_A < C_C$, $p = 0$). Thus, the mixed-strategy pair $(\sigma_i, \sigma_j) = ((\phi$ if malicious, C if regular), $p)$ is a BNE for the corresponding situations.

Therefore, the BNE of the stage game can be summarized as follows: When $\theta \leq (G_C - C_C)/(G_C + G_A)$, $(\sigma_i, \sigma_j) = ((A$ if malicious, C if regular), $C)$; after $\theta > (G_C - C_C)/(G_C + G_A)$, j becomes more conservative, and $(\sigma_i, \sigma_j) = ((\phi$ if malicious, C if regular), $p)$.

We obtain some conclusions by analyzing the stage game: 1) We analyze the stage games without considering the R and F options, and 2) the equilibrium of the regular/malicious node game should be constructed based on the BNE of the stage game.

We only need to consider C and A/D when searching for the BNE of a single stage game. However, the regular node has an additional option R, and the malicious node has an additional option F, which makes the sequential rationality more complicated.

D. Sequential Rationality: Report

If a regular node j decides to choose R in a stage, there are two possible results: 1) i is malicious, and the report is correct, and 2) i is regular, and the report is a false alarm.

The second result may occur since regular nodes also play D in some stage games to maximize their utility. Such a false

alarm would draw unnecessary attention and reduce regular nodes' sensitivity to real attacks. Therefore, regular nodes should estimate the loss L_F for the event of the false alarm. L_F is a subjective value that reflects the regular node's characteristic. Larger L_F indicates a more conservative characteristic. L_F is the private information of the regular node.

The regular node j's decision depends on the comparison between the expected correct report gain and the expected false alarm cost. Aside from the formed belief θ, j also needs to evaluate the sufficiency of the evidence before making decisions. We use uncertainty u to measure the sufficiency of evidence.

In regular nodes' reporting rule, which shares similar ideas with the sequential hypothesis testing theory, the threshold policies should be applied to achieve the optimal result. Regular node j decides whether to report in the current stage game by checking whether a threshold T has been reached. The threshold T should reflect the combined requirement on both the proportion of detected A/D in the evidence and the sufficiency of the evidence. Consider a case where $\alpha = 1$ and $\beta = 2$. Although $\theta = 0.67$ is high, the sufficiency of evidence is low. If we use a T that only focuses on θ, it is highly possible that a regular-type node i is falsely reported in this case. Since $1 - u$ can be regarded as regular node j's certainty toward the current evidence, $\theta \cdot (1 - u)$ is the proportion of certainty which supports the proposition that node i is a malicious node. The threshold T should be imposed on $\theta \cdot (1 - u)$ to reflect both requirements.

To satisfy the sequential rationality, node j should report only when $E_j(R) > \max\{E_j(C), E_j(D)\}$, where $E_j(R) = \theta \cdot (1 - u) \cdot (G_R - C_R) - ((1 - \theta) \cdot (1 - u) + u) \cdot (L_F + C_R)$. j should not choose R when $E_j(C) > 0$, as it should not end the game when it still expects to gain in the following stage games. Therefore, T should be calculated as a condition that makes $E_j(R) > 0$. We get $T = (L_F + C_R)/(G_R + L_F)$. When $\theta \cdot (1 - u) > (L_F + C_R)/(G_R + L_F)$, regular node j will choose R.

Assuming $T = 0.42$, when $\alpha = \beta = 10$, j should report as $\theta \cdot (1 - u) = 0.43 > T$. Consider the case where $\alpha = \beta = 2$. j should not report as $\theta \cdot (1 - u) = 0.2 < T$, although θ is the same. As the evidence is insufficient, R has a good chance of leading to a false alarm in the latter case.

E. Sequential Rationality: Flee

By using a threshold T as the decision rule for R and the mixed strategy to play C or D, we get the complete strategy profile for the regular node. In this section, we need to complete the strategy profile for the malicious node. More specifically, one question needs to be answered: when to flee?

When a malicious node decides to flee, the expected gain is to avoid the risk of being caught. However, what is the definition for the risk? Since i's attack frequency ϕ depends on node j's belief θ and j's reporting rule depends on belief and uncertainty, the malicious-type node i's risk should be calculated based on opponent j's current opinion and threshold. The risk is defined as the expected loss of being reported $Risk = P(catch) \cdot G_R$, where $P(catch)$ denotes the probability of being caught. The malicious node should check whether $E_i(F) = Risk - C_F > \max\{E_i(A), E_i(C)\}$. If this condition is satisfied, the malicious node should flee.

As the malicious-type node i has perfect information about the transaction history between itself and regular node j, it can precisely estimate j's belief toward it. Since L_F is a subjective cost for the false alarm of node j, node i cannot know the exact value of L_F. However, node i would have enough knowledge about the network and know the distribution of L_F. If the number of nodes is large enough in the network, L_F should comply to the normal distribution. Node i could know the standard deviation $VAR(L_F)$ and the expected value $E(L_F)$. $P(catch)$ is equal to the probability that the current $\theta \cdot (1 - u)$ will pass j's threshold T, and $P(\theta \cdot (1 - u) > T) = P(L_F < (\theta \cdot (1 - u) \cdot G_R - C_R)/(1 - \theta \cdot (1 - u)))$. Therefore, we have

$$P(catch) = \Phi\left(\frac{\frac{\theta \cdot (1-u) \cdot G_R - C_R}{1 - \theta \cdot (1-u)} - E(L_F)}{VAR(L_F)}\right) \tag{2}$$

where $\Phi(x) = (1/\sqrt{2\pi}) \int_{-\infty}^{x} \exp(-(u^2)/2)\mathrm{d}u$.

Assume that $T = 0.42$, $G_R = 100$, and $C_F = 10$. Without the F strategy, malicious-type node i needs to keep $\phi < 0.42$, or it can choose a higher ϕ and bear the loss of G_R. For example, if i chooses $\phi = 0.66$, it will be reported and lose 100 when $\alpha = 2$ and $\beta = 5$. With the F strategy, i could flee when $\alpha = 2$ and $\beta = 4$ by paying only ten.

From the analysis of the F strategy, we can see that the malicious node enjoys its advantage of choosing its optimal ϕ to attack and escaping punishment with the option to flee. It needs to keep evaluating the risk of staying and playing and find a tradeoff between risk and C_F to maximize its payoff.

Algorithm 1 Player j's PBE strategy σ_j^*
1: while $\theta \cdot (1 - u) < T$ **do**
2: **if** $\theta \leq (G_C - C_C)/(G_C + G_A)$ **then**
3: Choose C with $p = 1$;
4: **else**
5: Choose C with $p = (C_A - C_C)/G_A$;
6: **end if**;
7: Updated α, β, get θ and calculate u;
8: **end while**
9: Report node i as a malicious node;

Algorithm 2 Malicious-type player i's PBE strategy σ_i^*
1: while $E_i(F) < \max\{E_i(A), E_i(C)\}$ **do**
2: **if** $\theta \leq (G_C - C_C)/(G_C + G_A)$ **then**
3: Choose A with $\phi = 1$;
4: **else**
5: Choose A with $\phi = (G_C - C_C)/((G_C + G_A) \cdot \theta)$;
6: **end if**;
7: Track j's θ, estimate risk of being caught and $E_i(F)$;
8: **end while**
9: Flee to a remote area and attack again;

F. PBE

The PBE of this game describes the optimal decision rules for both regular and malicious nodes and reveals the connection between the best strategy profile and the cost and gain of individual strategies. From the discussion, we can summarize player j's PBE strategy σ_j^* as strategy profile 1. The regular-type player i has the same PBE strategy profile as j, and the PBE strategy σ_i^* of malicious-type player i is listed as strategy profile 2.

V. Countermeasures

The regular node needs to balance the possible loss for false alarm and gain in order to yield a correct report. It needs an evidence accumulation process to make a confident reporting decision. The malicious node clearly gains advantages by fleeing before the end of this process. Therefore, shortening the length of this process and making it less predictable become the networks' main countermeasures against malicious nodes.

A. Dynamic Threshold

Regular nodes can use a dynamic threshold to mitigate malicious nodes' threats. However, regular nodes cannot define their threshold T arbitrarily since this would violate the sequential rationality. A regular node will have a number of neighbors when it stays in one cluster. Through communicating with these nodes, it becomes more familiar with this cluster. The aforementioned L_F, which is the evaluated cost for the false alarm, decreases as it gains more confidence about its current cluster. The decrease of L_F leads to the decrease of T. This indicates that a regular node tends to be more aggressive in reporting as it learns more about the cluster that it stays in.

B. Belief Dissemination

In the aforementioned game, the flee strategy leads to a reputation reset with a 100% success probability. However, if this probability can be reduced, malicious nodes are forced to be more conservative. Malicious nodes tend to flee earlier, and the damage to the current cluster is reduced. If the node's identity binding cannot be changed in the MANET and the belief is disseminated among clusters as well, the aforementioned probability will be reduced.

To enforce identity binding in the MANET, a network-wide single authentication service with a strict identity policy should be used. Methods to thwart the sybil attack should also be employed to prevent faked identities. When a newcomer enters a cluster, a trusted node from that cluster will request the belief toward that node from all the other clusters.

We can also share belief within each cluster. In the game, regular nodes build their beliefs exclusively based on first-hand observations. This increases the detection time and makes their decisions more predictable. Malicious nodes play the game with each of their neighbors independently. Since regular nodes also observe each other and build up the trust, they can utilize this trust and share their beliefs.

VI. Discussion

In this section, we discuss several other possibilities related to the game theatrical analysis.

A. Regular Nodes With Tit-for-Tat

Tit-for-tat is a highly effective strategy in game theory for the iterated prisoner's dilemma. The regular nodes in the game may also adopt this strategy instead of using a belief system. The regular node will initially cooperate, then respond in kind to its neighbor's previous action. The advantage of this strategy is that regular nodes only need to remember the result of one stage game. However, the observation in wireless networks is not perfect. Although very rare, a regular forwarding of node i may be observed by a regular node j as D or F due to interference. Thus, the communication between regular nodes i and j will be disrupted forever because of tit-for-tat. The certainty-oriented belief system will be more robust toward the imperfect observation. Therefore, the certainty-oriented belief system will be a rational choice for regular nodes in a practical MANET environment.

Furthermore, the tit-for-tat strategy for regular nodes also leads to the interference attack from the malicious nodes. A malicious node only needs to interfere the communication among each pair of nodes once, and it can make the network completely noncooperative indefinitely.

B. Reputation System Without Uncertainty

Many reputation systems have been proposed in literature [15]–[17], [19]. Most of them sharply divide the recorded behavioral information into right or wrong. With these belief systems, a regular node j will have the same belief value in the case that i observed one A/D with one C from node i and the case that regular node j observed 100 A/D with 100 C from node i. The same belief makes the flee strategy and the PBE invalid. However, the two cases clearly have differences. While the first case may be caused by an imperfect observation, node j is more certain that node i is conducting an attack 50% of the time in the second case. Therefore, uncertainty is an unavoidable factor in the dynamic environment of MANETs. An uncertainty-aware analysis will be more practical in wireless networks.

C. Possible Equilibrium of Never Fleeing

When node j chooses the pure strategy C, the malicious-type node i can also follow the mixed strategy of C and A with a fixed low ϕ, where $\phi < (G_C - C_C)/(G_C + G_A)$. Since, in this case, $E_j(C) > E_j(D) = 0$, node j should always follow C and never choose R. However, whether the malicious-type node i wants to keep such a low attack frequency and benefits from this mixed strategy depends on the parameters. More specifically, a ϕ exists that makes $E_j(C) > 0$ and $E_i(\phi) \geq 0$ at the same time; regular and malicious nodes should follow $(\sigma_i^*, \sigma_j^*) = ((\phi \text{ if malicious}, C \text{ if regular}), C)$, which turns out

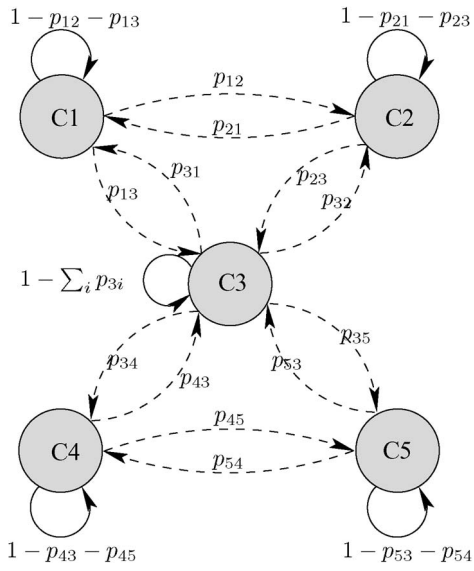


Fig. 3. Cluster-based mobility pattern for nodes in Fig. 1(a).

to be another possible equilibrium. The F and R strategies will not be used in this case, so the conditions are

$$\begin{cases} E_j(C) = \phi \cdot (-G_A - C_C) + (1-\phi) \cdot (G_C - C_C) > 0 \\ E_i(\phi) = \phi \cdot (G_A - C_A) + (1-\phi) \cdot (-C_C) \geq 0. \end{cases}$$

Hence, $\phi \in [C_C/(G_A - C_A + C_C), (G_C - C_C)/(G_A + G_C)) \neq \emptyset$; this equilibrium exists. The intuitive explanation for this equilibrium is that, when the cost for A and C is small enough and the gain is high, malicious nodes would like to afford small C costs to persuade the regular nodes to C most of the time and only A occasionally. The game repeats infinitely, and the malicious nodes will not flee. This indicates the situation that regular and malicious nodes may coexist in the MANETs. However, this equilibrium only exists when $C_C/(G_A - C_A + C_C) < (G_C - C_C)/(G_A + G_C)$. The PBE in this paper is more general and could be applied when this condition does not hold.

VII. Simulation

We conduct a simulation to evaluate the regular and malicious nodes' pure, mixed, and PBE strategy.

A. Simulation Setup

All proposed strategies have been implemented and compared on a custom discrete event simulator. All simulations are conducted in randomly generated MANETs. The regular node can track its neighbor's outgoing packets by neighbor monitoring.

One hundred nodes are randomly placed in a 900 m $\times$ 900 m region which is evenly divided into nine clusters. The transmission range is 250 m. Any two nodes within the same cluster are considered neighbors. Nodes follow the cluster-based mobility model [25]. Fig. 3 shows this mobility model for nodes in Fig. 1(a). The p_{xy} in Fig. 3 is the probability that regular nodes in cluster Cx will move to cluster Cy.

Each simulation is repeated 500 times, and the average data are used as the final result. The default number of malicious nodes is 40. The amount of energy for C_C is regarded as the unit cost/gain. We select the drop-packet attack as the sample attack in the simulation. The default values for the expected gain and cost parameters are $G_A = 20$, $G_C = 30$, and $G_R = 80$. L_F complies to the normal distribution with $E(L_F) = 100$ and $VAR(L_F) = 20$. The utility in the following figures shows the actual average payoff of nodes.

B. Simulation Results

In Fig. 4(a)–(d), malicious nodes always follow their PBE strategy. We record the results of different stage games to compare regular nodes' different strategy profiles. In Fig. 4(a) and (b), regular nodes' PBE strategy outperforms the other two strategies. From Fig. 4(a), we can see that, when regular nodes follow pure strategy C, their utility is high. This is due to the fact that regular nodes hold all the opportunities to cooperate with other regular nodes. However, it will surely stimulate the malicious nodes to attack. As shown in Fig. 4(b), the utility of the malicious nodes is the highest in this case.

Regular nodes can choose the mixed strategy σ_j: $\{p = (C_A - C_C)/G_A\}$ which makes $E_i(A) = E_i(C)$ for malicious nodes. This method greatly reduces malicious nodes' payoff. The corresponding curve in Fig. 4(b) shows that the utility for malicious nodes is negative. However, this mixed strategy is too conservative. While greatly reducing malicious nodes' utility, regular nodes' average utility is the lowest in Fig. 4(a).

Fig. 4(c) shows the convergence process of the estimated θ. As the estimated θ is mainly decided by the malicious nodes' strategy, the curves for the three cases are very close to each other. θ intensely vibrates in the earlier stages and converges in the later stages. Malicious nodes' periodic fleeing causes the vibration. When a malicious node attacks continuously at one location, θ goes up quickly. After it flees to a new destination, it attacks again with a clean history. As the malicious nodes' strategy selection becomes more diverse in later stages, the regular nodes' belief converges.

In Fig. 5(a)–(d), regular nodes always follow their PBE strategy. We compare malicious nodes' different strategies, and the PBE strategy outperforms the others. In Fig. 5(a) and (b), when malicious nodes exploit pure strategy A or mixed strategy ϕ, they can only affect regular nodes' utility in the first several stages, and their utility drops dramatically.

Fig. 5(c) shows the connection between the malicious nodes' strategy and the variation of the regular nodes' belief. When the malicious node follows pure strategy A, the estimated θ should converge to 100% in the first few stages. When the malicious node exploits the mixed strategy ϕ, it is more deceptive. We can see that the curve for the mixed strategy has a ladder shape. However, the malicious node will still be reported. When applying the PBE strategy, the malicious node has a good chance of escaping being reported by fleeing.

Figs. 4(d) and 5(d) show the uncertainty u in the aforementioned two cases. The tendency of the curves is just opposite to those in Figs. 4(c) and 5(c). This proves that uncertainty is the determinant element of regular nodes' decision.

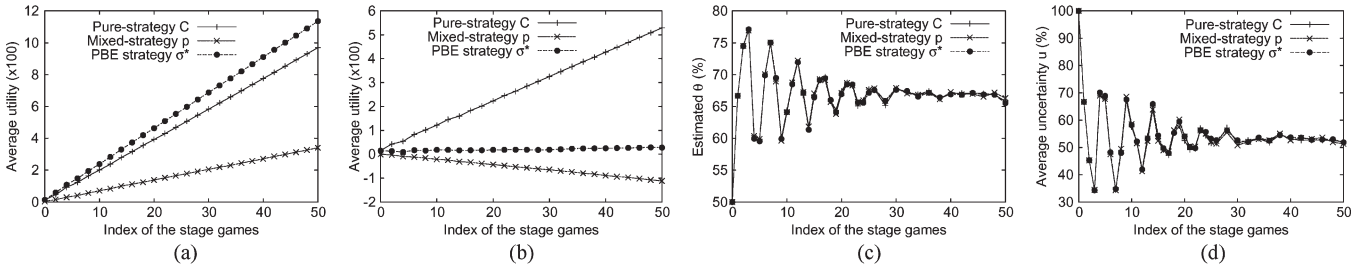


Fig. 4. Regular nodes' strategy comparison when malicious nodes follow their PBE strategy. (a) Regular nodes' utility. (b) Malicious nodes' utility. (c) Belief. (d) Uncertainty.

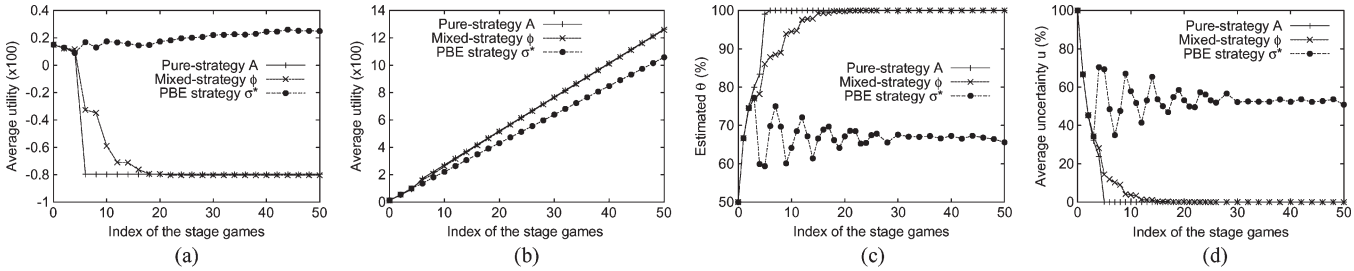


Fig. 5. Malicious nodes' strategy comparison when regular nodes follow their PBE strategy. (a) Malicious nodes' utility. (b) Regular nodes' utility. (c) Belief. (d) Uncertainty.

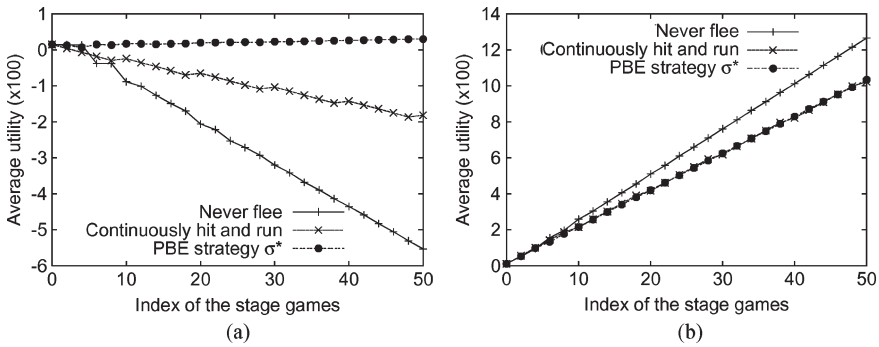


Fig. 6. Flee strategy comparison. (a) Malicious nodes' utility. (b) Regular nodes' utility.

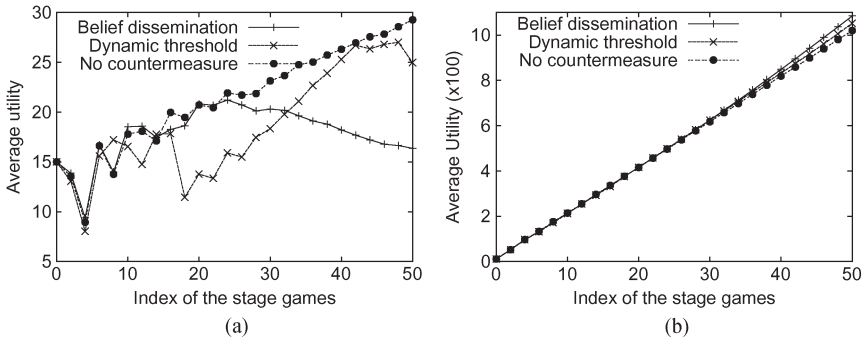


Fig. 7. Countermeasure comparison. (a) Malicious nodes' utility. (b) Regular nodes' utility.

In Fig. 6(a) and (b), we compare different methods of fleeing. The first is never fleeing. Malicious nodes could only select $\phi < (G_C - C_C)/(G_C + G_A)$ or increase ϕ but bear the loss of being caught. The latter case is shown in Fig. 5. For the former case, the average utility of the regular nodes is the highest in Fig. 6(b) as malicious nodes can only choose a low ϕ to attack. Moreover, the average utility of the malicious node is the lowest in this case. The average utility of regular nodes is similar when malicious nodes follow the PBE strategy or continuously hit and run. However, the malicious nodes' utility is much higher in the PBE-strategy case. Therefore, following the PBE strategy outperforms other flee options.

Fig. 7(a) and (b) demonstrates the effectiveness of the proposed countermeasures. Using the intercluster belief dissemination or the dynamic threshold method (combined with intracluster belief sharing), the utility of the malicious node

is reduced. However, both methods rely on the regular nodes' mobility model and organization.

The simulation results can be summarized as follows: 1) The PBE strategies for both parties are better than other pure or mixed strategies; 2) regular nodes' decision rules, which consider the evidence sufficiency, balance the possible gains from cooperation with regular nodes and the threats from malicious nodes; and 3) the flee strategy is one key point for the malicious nodes. It greatly increases the malicious nodes' utility.

VIII. Conclusion

In this paper, we used a dynamic Bayesian game framework to analyze the wrestling between regular and malicious nodes in mobile networks. The regular node forms belief, chooses the probability to cooperate with its opponent based on its belief, and follows a rational decision rule to report. The malicious node keeps evaluating the risk of being caught and exploits its flee strategy to avoid punishment. We analyze the PBE in this game and emphasize the advantages that malicious nodes would gain from the flee strategy. Our future work will focus on multiattacker collusion in the regular/malicious node game. We are particularly interested in the scenario where attackers can come together in a locality to conduct sophisticated attacks.

Appendix

We first analyze the reason that the uncertainty should be measured. Then, we give formal proof of PBE in the regular/malicious node game.

Rationality of the Reporting Rule: We examine the $(k+1)$th stage game. Node j's current belief $\theta = \beta/(\alpha+\beta)$ is the prior probability of the decision. We assume that the average probability that malicious-type node i chooses A is ϕ, and the average probability that regular-type node i will choose D is $1-p$. The results of the previous k stage games should comply to the binomial distribution, and $k = \alpha + \beta - 2$. Therefore, $P((\alpha,\beta)|r) = \binom{k}{\beta-1}(1-p)^{\beta-1}p^{\alpha-1}$, and $P((\alpha,\beta)|m) = \binom{k}{\beta-1}\phi^{\beta-1}(1-\phi)^{\alpha-1}$, where r denotes regular and m denotes malicious.

Hence, the probability that the regular node's decision to report leads to a false alarm is

$$P(r|(\alpha,\beta)) = \frac{(1-\theta)\binom{k}{\beta}p^{\beta}(1-p)^{k-\beta}}{(1-\theta)\binom{k}{\beta}p^{\beta}(1-p)^{k-\beta} + \theta\binom{k}{\beta}\phi^{\beta}(1-\phi)^{k-\beta}}$$

and $P(m|(\alpha,\beta)) = 1 - P(r|(\alpha,\beta))$. As the sequential rationality condition for R is $P(r|(\alpha,\beta)) \cdot (L_F + C_R) \leq P(m|(\alpha,\beta)) \cdot (G_R - C_R)$, we can derive

$$\frac{k-\beta}{\beta}\left(\frac{1-p}{\phi}\right)^{\beta}\left(\frac{p}{1-\phi}\right)^{k-\beta} \leq \frac{(G_R - C_R)}{(L_F + C_R)}. \quad (3)$$

Inequality (3) reflects that both β's proportion of k and the value of k must be considered. Hence, we get Lemma 1.

Lemma 1: Based only on the belief θ, a threshold-based reporting policy cannot guarantee the sequential rationality for regular nodes.

Proof: If we take only the belief into account when imposing the threshold without considering uncertainty, the decision rule becomes $\beta/(\alpha+\beta) > T$, and the regular node should report.

The threshold T in the decision rule regulates only the relationship between α and β, where $\beta \geq (T/(1-T)) \cdot \alpha$. T cannot regulate the value of k, which reflects the sufficiency of observations. It violates the sequential rationality requirement reflected in (3). ■

Therefore, only measuring the belief is not enough for the sequential rationality requirement. Theorem 1 states that a combined threshold on uncertainty u and belief θ is necessary.

Theorem 1: By imposing a threshold T on $\theta \cdot (1-u)$, the sequential rationality for regular nodes can be guaranteed.

Proof: By imposing the threshold T on disbelief d, we impose a combined requirement on both u and $\beta/(\alpha+\beta)$. As $(\beta/(\alpha+\beta)) \cdot (1-u) > T$, we have $u = (12 \cdot \alpha \cdot \beta)/((\alpha+\beta)^2 \cdot (\alpha+\beta+1)) \leq 1 - T$ according to (1). Hence

$$\frac{12 \cdot \alpha^2 \cdot T \cdot (1-T)}{\alpha^2 \cdot (1-T+T)^2 \cdot (k+3)} \leq 1 - T \quad (4)$$

which leads to $k > 12 \cdot T - 3$ as $\beta \geq (T/(1-T)) \cdot \alpha$. Therefore, we now have a combined requirement for both the proportion of evidence for A/D and the sufficiency of observations. ■

Optimality of Strategy Profiles (σ_i^*, σ_j^*): We first prove that the regular/malicious node game has a PBE since the game satisfies the Bayesian postulates. After that, we prove that both the proposed PBE strategy profiles 1 and 2 satisfy the sequential rationality condition.

Lemma 2 (Bayesian Postulates): The described game satisfies the following four Bayesian conditions [6].

- B1) Posterior beliefs are independent. All types of receivers have the same beliefs.
- B2) Bayes' rule is used to update beliefs (θ) from stage game k to stage game $k+1$ whenever possible.
- B3) The players do not signal what they do not know.
- B4) All players must have the same belief about the type of another player.

Proof: B1 is satisfied because receiver j has only one type which is regular. Since $\theta = \beta/(\alpha+\beta)$, the updated θ satisfies Bayes' rule when α or β is incremented. Hence, B2 is satisfied. The regular and malicious nodes select their signal (A/D or C) based on their own payoff, which fulfills B3. Because there are only two players in the game and no other players influence the belief updates, B4 is satisfied. ■

Lemma 3 (Sequential Rationality): For each player x, given any alternative strategy σ_x of x, σ_x^* satisfies $E_x(\sigma_x^*) \geq E_x(\sigma_x)$. Here, $E_x(\sigma_x)$ denotes the expected payoff of x's strategy σ_x when other players play best response to σ_x.

Proof: As the receiver of the game, regular node j plays R only when $E_j(R) > \max\{E_j(C), E_j(R)\}$. Otherwise, it will play C with the optimal probability p. The actions of the receiver maximize its expected payoffs given its beliefs.

Similarly, the sender i, which could be a malicious or a regular node, chooses to A/D or C depending on which action will maximize its payoff given j's strategy and its own type. ■

As stated in [6], Theorem 2 can be derived from Lemmas 2 and 3, which indicates that (σ_i^*, σ_j^*) are the optimal decision rules for both parties in this game.

Theorem 2: (σ_i^*, σ_j^*) described by strategy profiles 1 and 2 is a PBE of the regular/malicious node game.

Proof: Since the described regular/malicious node game satisfies the Bayesian conditions B1–B4 (Lemma 1) and (σ_i^*, σ_j^*) described by strategy profiles 1 and 2 satisfies the sequential rationality condition (Lemma 2), (σ_i^*, σ_j^*) is a PBE. ■

REFERENCES

[1] A. Blanc, Y. Liu, and A. Vahdat, "Designing incentives for peer-to-peer routing," in *Proc. IEEE INFOCOM*, 2005, pp. 374–385.

[2] L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, Oct. 2003.

[3] M. Felegyhazi, J. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 5, pp. 463–476, May 2006.

[4] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives and strategies," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 78–118, Feb. 2005.

[5] G. Theodorakopoulos and J. Baras, "Malicious users in unstructured networks," in *Proc. IEEE INFOCOM*, 2007, pp. 884–891.

[6] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.

[7] R. Axelrod and W. Hamilton, "The evolution of cooperation," *Science*, vol. 211, no. 4489, pp. 1390–1396, Mar. 1981.

[8] P. Nuggehalli, M. Sarkar, K. Kulkarni, and R. Rao, "A game-theoretic analysis of QoS in wireless MAC," in *Proc. IEEE INFOCOM*, 2008, pp. 1903–1911.

[9] S. Ng and W. Seah, "Game-theoretic model for collaborative protocols in selfish, tariff-free, multihop wireless networks," in *Proc. IEEE INFOCOM*, 2008, pp. 216–220.

[10] S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, "Information concealing games," in *Proc. IEEE INFOCOM*, 2008, pp. 2119–2127.

[11] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling smart jammers using multi-layer agility," in *Proc. IEEE INFOCOM*, 2007, pp. 2536–2540.

[12] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. ACM GameNets*, 2006, p. 4.

[13] L. Chen and J. Leneutre, "Selfishness, not always a nightmare: Modeling selfish MAC behaviors in wireless mobile ad hoc networks," in *Proc. IEEE ICDCS*, 2007, p. 16.

[14] S. Buchegger and J. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop Econ. Peer-to-Peer Syst.*, 2004, pp. 403–410.

[15] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. Commun. Multimedia Secur.*, 2002, pp. 107–121.

[16] S. Buchegger and J. Boudec, "Performance analysis of the confidant protocol," in *Proc. ACM MobiHoc*, 2002, pp. 226–236.

[17] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford Univ. Press, Stanford, CA, Tech. Rep. (CoRR cs.NI/0307012), 2003.

[18] F. Li and J. Wu, "Mobility reduces uncertainty in MANETs," in *Proc. IEEE INFOCOM*, 2007, pp. 1946–1954.

[19] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[20] F. Li, A. Srinivasan, M. Lu, and J. Wu, "Uncertainty mitigation for utility-oriented routing in MANETs," in *Proc. IEEE GLOBECOM*, 2007, pp. 427–431.

[21] F. Li and J. Wu, "Hit and run: A Bayesian game between malicious and regular nodes in mobile networks," in *Proc. IEEE SECON*, 2008, pp. 432–440.

[22] V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, "Cooperation in wireless ad hoc networks," in *Proc. IEEE INFOCOM*, 2003, pp. 808–817.

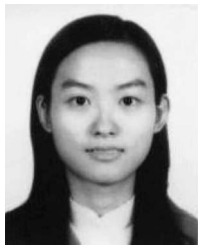
[23] E. Altman, A. Kherani, P. Michiardi, and R. Molva, "Non-cooperative forwarding in ad hoc networks," INRIA, Sophia-Antipolis, France, Tech. Rep. RR-5116, 2004.

[24] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom*, 2000, pp. 255–265.

[25] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling time-variant user mobility in wireless mobile networks," in *Proc. IEEE INFOCOM*, 2007, pp. 758–766.

Feng Li (M'05) received the Ph.D. degree in computer science from Florida Atlantic University, Boca Raton, in 2009, where his Ph.D. advisor is Prof. Jie Wu.

Since August 2009, he has been with the Department of Computer, Information, and Leadership Technology, Indiana University-Purdue University Indianapolis, Indianapolis, as an Assistant Professor. His research interests include the areas of wireless networks and mobile computing, security, and trust management. He has published more than 20 papers in conferences and journals.



Yinying Yang (S'08) is currently working toward the Ph.D. degree in the Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, under the supervision of Dr. Mihaela Cardei.

Her research interests mainly focus on wireless sensor networks, mobile computing, computer networking, parallel, and distributed systems.

Jie Wu (F'09) received the Ph.D. dgree in computer engineering from Florida Atlantic University in 1989.

He was the Program Director with the U.S. National Science Foundation. He is currently the Chairman and a Professor with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA. His research interests include the areas of wireless networks and mobile computing, routing protocols, fault-tolerant computing, and interconnection networks. He has published more than 450 papers in various journals and conference proceedings.

Dr. Wu serves in the editorial board of the IEEE TRANSACTIONS ON MOBILE COMPUTING. He was also the General Cochair for IEEE MASS'06, IEEE IPDPS'08, and DCOSS'09. He has served as an IEEE Computer Society Distinguished Visitor and is the Chairman of the IEEE Technical Committee on Distributed Processing.