IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 27, 2019, accepted December 5, 2019, date of publication December 19, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2961059

Misbehavior Detection in Ephemeral Networks: A Local Voting Game in Presence of Uncertainty

ALI BEHFARNIA, (Student Member, IEEE), AND ALI ESLAMI, (Member, IEEE)
Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260, USA

Corresponding author: Ali Behfarnia (axbehfarnia@shockers.wichita.edu)

This work was supported in part by the National Science Foundation under Grant OIA-1656006 and in part by the State of Kansas through the Kansas Board of Regents.

ABSTRACT Emerging short-lived (ephemeral) connections between wireless mobile devices have raised concerns over the security of ephemeral networks. An important security challenge in these networks is to identify misbehaving nodes, especially in places where a centrally managed station is absent. To tackle this problem, a local voting-based scheme (game) in which neighboring nodes quickly decide whether to discredit an accused (target) node in mobile networks has been introduced in the literature. However, nodes' beliefs and reactions significantly affect the outcome of target node identification in the collaboration. In this paper, a plain Bayesian game between a benign node and a target node in one stage of a local voting-based scheme is proposed in order to capture uncertainties of nodes for target node identification. In this context, the expected utilities (payoffs) of players in the game are defined according to uncertainties of nodes regarding their monitoring systems, the type of target node and participants, and the outcome of the cooperation. Meanwhile, incentives are offered in payoffs in order to promote cooperation in the network. To discourage nodes from abusing incentives, a variable-benefit approach that rewards each player according to the value of their contribution to the game is introduced. Then, possible equilibrium points between a benign node and a malicious node are derived using a pure-strategy Bayesian Nash equilibrium (BNE) and a mixed-strategy BNE, ensuring that no node is able to improve its payoffs by changing its strategy. Finally, the behavior of malicious and benign nodes is studied via simulations. Specifically, it is shown how the aforementioned uncertainties and the designed incentives impact the strategies of the players and, consequently, the correct target-node identification.

INDEX TERMS Misbehavior detection, local voting-based scheme, game theory, uncertainty, ephemeral networks.

I. INTRODUCTION

A. MOTIVATION

The proliferation of temporal peer-to-peer communication between wireless devices gives rise to the formation of short-lived (ephemeral) networks due to the unpredictable existence of mobile nodes. Ephemeral networks are pervasive over a variety of applications, such as vehicular ad hoc networks, mobile social networks, wireless sensor networks, etc. [2]–[5]. These networks are attractive to malicious nodes so they join and manipulate sensed data, thereby influencing network performance [6]. For example, in the case of vehicular ad hoc networks (VANETs), a malicious vehicle can inject false information to its neighbors and trigger a serious problem on the road. In addition to data manipulation or sending false information, a malicious node can compromise the vehicle's routing efficiency by not forwarding the packets that it received in the network. Therefore, an important security improvement in ephemeral networks is to reveal the type of nodes, either benign or malicious, especially in places where centrally managed stations are absent. In such transitory distributed networks, quick cooperation among neighboring nodes can provide effective solutions toward improving network performance [7], [8]. However, nodes are usually selfish and reluctant to cooperate, simply because they must use their resources. In addition, each node has some inherent uncertainties in a collaboration, including the type of participants, the accuracy of its own components (e.g., detection system), the value of its contribution, and attainable outcomes, all of which affect the node's decision about whether to participate.

The associate editor coordinating the review of this manuscript and approving it for publication was Walid Al-Hussaibi.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

In this respect, it is crucial to provide incentives according to different reactions of nodes under uncertainty in order to achieve malicious-node detection.

B. RELATED WORK

A variety of precise and effective schemes have been proposed to detect misbehaving nodes. The authors in [9] [10] have provided a comprehensive literature review on misbehavior detection in cyber-physical systems (CPSs) and intelligent transportation systems, which covered a variety of solutions for transient networks wherein nodes have different limitations. In particular, Liu *et al.* [11] studied the interactions between an attacker and a defender in order to detect misbehaving nodes in ad hoc networks. They considered scenarios where a malicious node can either attack or not attack a benign node, while the defender may be in a monitoring or non-monitoring state. The interactions between players were analyzed by game theory, which is a powerful tool to obtain the best strategies of independent decision makers [12]. Although this paper clearly described the individual interactions and uncertainties between two agents, it did not consider the identification of a misbehaving node for all nodes in the network. Another approach for misbehavior detection is to use reputation systems for which a history of credits is built for nodes based on their past behavior in the network. However, this method needs a database that can be created over time, and nodes may have to continuously monitor their neighbors [13]. Considering short time connections between nodes, reputation systems do not appear to be a proper approach in ephemeral networks [14].

In other work, a local revocation process is introduced to consider the dynamic nature of ephemeral networks [14]–[21]. In the revocation process, a benign node as an initiator is assumed to detect (or become suspicious of) a malicious node and broadcasts its identification (ID) as a *target node* or an accused node. Then, other benign neighboring nodes run a local voting-based scheme to decide whether to discredit the target node. Scholars in [14]–[16] studied the local revocation process as a sequential voting game in which a benign node can choose one of three strategies with regard to (w.r.t.) a target node: voting, abstaining, or self-sacrificing. A benign node chooses between a voting strategy or an abstaining strategy based on its economic considerations in the game. Also, the benign node might use a self-sacrificing strategy to declare the invalidity of its current identity as well as the identity of the target node. Some limitations of the proposed revocation process in vehicular ad hoc networks (VANETs) have been pointed out by Liu *et al.* [16]. For example, they underlined the assumption of complete information for nodes in the game and proved that the identification of the target node may not be possible without considering the rate of false positives and the rate of false negatives.

To address existing problems and introducing new approaches for misbehavior detection in mobile networks, Abass *et al.* [17] introduced an evolutionary game wherein all benign nodes cooperate in the voting game, focusing on unsuccessful revocation and over-reacted revocation decisions. Scholars [18], [19] have developed a weighted voting game based on clustering architecture to effectively solve the problem of false accusation. Masdari [20] proposed a collaborative false accusation approach to stop wrong accusations in the network. Diakonikolas and Pavlou [22] emphasized the inverse power index problem in designing weighted voting games and proved that the problem is computationally intractable for a broad family of semi-values. In another work, Subba *et al.* [23] proposed an intrusion detection system (IDS) that employs the concept of election leaders and a hybrid IDS, with the aim of avoiding the continuous monitoring of nodes in mobile ad hoc networks (MANETs). These authors then extended their work in [24] by providing a multi-layer game theory to address the problem of dynamic network topologies in VANETs. While these efforts are effective at minimizing the volume of IDS traffic, they do not address the uncertainty of nodes alongside incentives in local voting games. Others [25] have studied the impact of incentives on misbehavior detection in unmanned aerial vehicle (UAV)-assisted VANETs. Silva *et al.* [26] proposed a voting scheme to generate a large set of novel strategies from available expert-based ones. The proposed scheme selects the best strategies while the model of opponents are considered during the game. However, this work does not focus on identifying a malicious node in an ephemeral network.

C. NOVELTIES AND CONTRIBUTIONS

Some differences distinguish this paper from other significant contributions in the literature. First, we design a local voting game wherein the type of target node can be either malicious or benign. This is in contrary to several papers [15], [17], [20], in which authors presume that a benign initiator broadcasts the ID of a malicious node as the target node. The reason of our assumption is that every node, including malicious nodes, can accuse others and all benign nodes do not necessarily need to know each other in the network. In our design, nodes vote regarding the type of target node based on the accuracy and cost of their monitoring systems as well as a pre-defined belief about the portion of malicious nodes in the network. These considerations provide a framework in which nodes look at their resources and potential hostile environments before taking part in the voting game. Second, we consider that benign nodes are uncertain about the strategy of malicious nodes in the network. This is because a malicious node might intentionally not attack a benign node in order to obtain its support during the local voting game. This point is omitted in the design of the local voting game in [14]–[20]. In particular, these works mainly focused on target node identification based on the rate of participation rather than considering the malicious node strategy of avoiding being accused. Third, we design incentives to encourage only knowledgeable nodes (i.e., nodes that have already monitored the target node) in the game. Otherwise, the incentives lead to many random votes in the game, which might spoil the result

of cooperation. This point is mostly overlooked in the above literature, and [27] that studied the role of nodes' incentives in order to contribute to ephemeral social networks. Fourth, we consider that both benign nodes and malicious nodes can take part in the voting game. This implies that a benign node cannot rely solely on others' votes, owing to misleading votes from malicious nodes. The incomplete information of nodes in voting was not studied in the above literature, including [14], [17], [20]. Fifth, the cost of a group participating in the game (a.k.a., social cost) should be designed based on nodes' contributions and their uncertainties about the results. For example, a cooperative node should be punished less than an abstaining node when the collaboration becomes unsuccessful. Finally, a potent design should provide more rewards for decisive votes. Although some authors studied weighted voting games [19], [28], they mainly based their designs on clustering heads rather than the value of a vote in the middle of a local voting games.

We implement the points above in analyzing misbehavior detection using the local voting-based scheme in the presence of uncertainty. Our main contributions in this paper can be summarized as follows:

- We provide a game layout between a benign player and a target node in one stage of a local voting game using a static Bayesian game in order to detect misbehaving nodes in an ephemeral network. In this regard, we design expected utilities (payoffs) that capture uncertainties (explained above) regarding detection systems, types of participants, type of target node, and outcome of the game. We also offer incentives in node payoffs in order to promote cooperation in the network. Furthermore, we introduce a variable benefit for cooperative nodes in which rewards are adjusted according to the value of contributions in the game. This scheme prevents nodes from abusing incentives by pointless participation.
- We derive possible equilibrium points between a benign player and a target node in the game using a pure-strategy Bayesian Nash equilibrium BNE) and a mixed-strategy BNE, ensuring that no node can improve its utility by changing its strategy. The best strategies can be adopted by malicious nodes and benign nodes w.r.t. different game parameters.
- We provide extensive numerical results to verify the analysis and investigate the impact of cooperation parameters and uncertainties on the identification of malicious nodes. Our results confirm the influence of the designed incentives, hence participation rate, on the strategies of malicious and benign nodes in an ephemeral network. We observe, in particular, that if the participation incentives go beyond a certain limit, then *correct* target-node identification will be decreased, in spite of the growing participation rate.

D. PAPER ORGANIZATION

The remainder of this paper is organized as follows. Section II describes assumptions, the local voting game, and the objectives of this paper. Section III formulates the game, including defining parameters, payoff design, and a variable benefit scheme. Section IV applies Bayesian game analysis to derive equilibrium points in the proposed model. Section V is devoted to extensive numerical results. Section VI concludes the paper.

II. ASSUMPTIONS AND PROBLEM DESCRIPTION

A. NETWORK MODEL

We study misbehavior detection in a network where nodes have short-lived connections, and a centrally managed station is absent. We use a vehicular ad hoc network (VANET) as a typical example of an ephemeral network to explain our approach. We assume that nodes (e.g., vehicles) are powerful enough to have wireless communication among themselves. We consider a contention-based medium, e.g., IEEE 802.11p in a VANET, which can represent the nature of wireless channel access [14]. We further assume that a base station or a certificate authority has already established the credential of the nodes; hence, each node has a unique ID.

We assume that there are two types of nodes in the network: malicious and benign. Malicious nodes may attack benign nodes by disseminating false information. For example, a malicious car might inject faulty data to the sensors of the car that follows it, in order to manipulate an optimal space between them [29]. On the other hand, a benign node is equipped with a monitoring system to detect abnormal or counterfeit signals. For example, an autonomous vehicle can use a set of anti-spoofing techniques to detect fake global positioning system (GPS) signals [30]. However, benign nodes do not necessarily need to monitor all of their neighbors, due to the cost of monitoring over all short-lived connections.

B. LOCAL VOTING GAME

Nodes can participate in a local voting-based scheme (game) in order to determine the identity of a node in the network. The voting game starts when an initiator broadcasts the ID of a target node. Then, neighboring nodes choose either to vote or not to vote (abstain) on type of the target node. Each node calculates its costs and benefits in order to choose a strategy. Nodes can broadcast their decisions sequentially, and each node's decision is made in one stage of the game. We assume that the belief of a node w.r.t. the target node is independently inferred and does not change (e.g., by other votes) during the game. This is because nodes are uncertain about the correctness of other votes. In other words, a node may not know the types of all previous nodes that have already voted. Also, the node is unaware of the target node's strategy w.r.t. previous nodes. Hence, we assume that a node votes based on its own detection system. It is worth noting that monitoring all neighboring nodes and their interactions might be too costly for a node in an ephemeral network. The target node is identified when the number of votes in one type (either malicious or benign) reaches a pre-defined number. This number is denoted by n_{th} and is studied in

section V-B. If correct (wrong) votes reach n_{th}, then we will have correct (wrong) target node identification. If n_{th} is not reached during the game, then we will have *undecided* target node identification.

Malicious nodes and benign nodes can choose some strategies in the game. A malicious node can select to attack or not to attack a benign node, while it is unaware of being monitored. After a target node is determined, a benign node checks whether it has already monitored the target node. If it has not monitored the target node, it will abstain from voting, simply because it does not have any information about the node. But, if the benign node has monitored the target node, it will calculate its payoffs. If its voting payoff outweighs its abstaining payoff, then the benign node will vote; otherwise, it will abstain. On the other hand, malicious nodes vote against a benign target node and for a malicious target node. If there is no possibility for malicious nodes to change the result of the game in their favor, then they abstain from voting. We do not consider strategic malicious nodes that can optimize their types of votes to collect some credits or to send multiple wrong votes (e.g., Sybil attack [31]).

C. PROBLEM DEFINITION

Fig. 1 shows an example of a local voting game in a VANET that helps us explain the problem. As can be seen, nodes 0, 2, and 5 are malicious, and the other nodes are benign. We assume that node 0 is the target node and $n_{th} = 2$. We also assume that node 1 casts a correct vote, and node 2 casts a wrong vote. Now, node 3 should reveal its strategy. Here, we study the possible reactions of node 3 (as an example of a benign node) in the game where identification of the target node is not yet finalized. If node 3 has not monitored node 0, then it simply abstains. Otherwise, if it has already monitored node 0, it can select between voting or abstaining. To choose its strategy, node 3 faces some uncertainties that greatly impact its decision.

The first uncertainty of node 3 is about its own monitoring system, which has a predefined detection rate and false alarm rate. For example, the monitoring system of node 3 might recognize node 0 as benign, even though it is malicious. Next, node 0 might choose not to attack node 3 in order to produce a wrong perception. Hence, node 3, even if not attacked by node 0, would still be uncertain about the type of node 0. In addition, node 3 might not have monitored nodes 1 and 2; hence, it cannot vote based on previous votes. Moreover, node 3 may not have monitored all remaining nodes in the voting game, so it cannot count on their correct votes. This implies that the node is also uncertain about the outcome of the game, which potentially affects its decision. Nevertheless, incentives should be offered to encourage node 3 (and others) in cooperation. This could also avoid the formation of free-riders (i.e., nodes that benefit from the results without making any contributions [32]) in the network. It is worth noting that, depending on the stage of the game, a node's strategy could make a different level of impact on the results. For instance, if node 3 abstains, then the vote of node 4 is absolutely necessary for correct target identification ($n_{th} = 2$). Hence, incentives should be offered w.r.t. the value of a contribution.

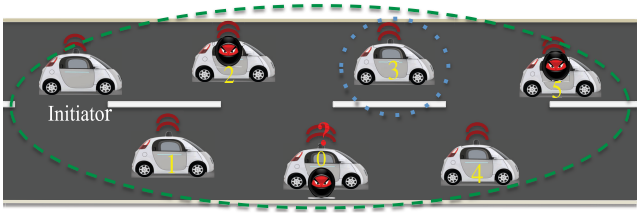

FIGURE 1. Example of local voting game in VANETs.

On the other hand, malicious nodes are aware of an existing voting game in the network. That is, a malicious node knows that it might become a target node. The objective of a malicious node is to maximize the level of its aggressiveness in the network without being identified. However, it is uncertain about being monitored by a benign node, and the strategy of a benign node in the game (i.e., voting or abstaining). In contrast, a benign node knows that some of its neighbors may be malicious. The objective of a monitoring benign node is to choose a strategy with the aim of target node identification. However, a benign node has some limitations in its detection system. Also, it is uncertain about the strategies of malicious nodes and, therefore, is uncertain about the type of the target node. Taking these points into consideration, our goal is the following:

- To design payoffs for a benign node w.r.t. the explained uncertainties and the value of its contribution in the game,
- To determine the best strategies for malicious nodes and benign nodes.

We address the first problem in section IV by considering the following: (i) the vote of a benign node that could be either correct or incorrect; (ii) the probability of correct target node identification in each stage, which is mainly based on votes that have already been cast; and (iii) the impact of a benign node's strategy on correct, wrong, and undecided target node identification. We address the second problem in section V. In particular, we develop one stage of the voting game as a Bayesian game to study the reactions of a benign node w.r.t. a target node. This helps us understand the best strategies of both types of nodes in the network.

To find the best strategies of players in the game, one could employ the concept of subgame perfect equilibrium, wherein nodes have complete information in a sequential game. However, as explained above, complete information does not seem to be a realistic assumption for nodes in an ephemeral network. Hence, we do not apply this concept to our model. Another solution is to use the concept of perfect Bayesian equilibrium (PBE) in dynamic Bayesian games to capture the incomplete information of nodes. In this context, a node needs to update its belief regarding its opponent's type according to the game evolution. However, we believe that the belief of a benign player regarding the type of target node

should not change by other votes during the game because of existing uncertainties about the types of neighboring nodes, their interactions, and the cost of monitoring over all neighbors in an ephemeral network. In principle, we assume that nodes are relying on their own detection systems to vote on the type of the target node. In this regard, we can not properly apply the concept of PBE to our model.

On the other hand, a Bayesian game is general enough to capture many scenarios between attackers and defenders in one stage of the game [32]. In particular, we can consider a potential attacker as a target node that chooses to attack or not to attack a benign node, and the benign player that can vote or abstain in one stage of the game. One advantage of applying Bayesian games to our model is that nodes independently infer the type of a target node using a detection system, and they do not need to know the type of all neighbors and their interactions with each other. In other words, a node can efficiently select its strategy according to the BNE that maximizes its expected utility with a set of parameters. However, one drawback of using BNE is that a benign node requires a sensible prior belief regarding the type of neighboring nodes. We let μ denote the prior belief of benign nodes about the portion of malicious nodes in a network (parameters are described in section III-A). In practice, a node should be able to adjust the values of μ according to its knowledge of an environment. Nodes could assign a high value for μ in potentially hostile places such as crowded areas in mega cities, and a low value for μ in safe places such as rural areas.

III. PROBLEM FORMULATION

In this section, we first introduce a set of parameters that are required to define the underlying game. Next, we provide some definitions to facilitate the explanation of our model. Then, we design payoffs that include individual beliefs and available voting information in the game. Finally, we propose a variable-benefit scheme that rewards participants according to the value of their contributions.

A. PARAMETERS

To describe our model, we need to define a set of given parameters to design player's payoffs in the game. We list these parameters in Table 1. To begin, we assume that a benign node holds an asset with a security value of w, where $w > 0$. This parameter is considered in order to count for the value of a vulnerable asset in benign nodes that can be exploited by malicious nodes. . A malicious node could compromise the asset by paying the cost of an attack, denoted by c_a. In contrast, a benign node protects its asset by monitoring for attacks, with probability P_m. This monitoring costs c_m for the node, and all costs are positive. It is rational to assume that $w > c_a$ and $w > c_m$. Otherwise, the attacker and the benign node lose their motivation to attack and to protect the asset, respectively. A benign node assigns a prior probability of μ for its neighbors to be malicious. We measure the performance of the monitoring system by considering the following: (i) α, which represents the detection rate (i.e., true positive rate), and (ii) β, which denotes the false alarm (i.e., false positive rate) for detecting abnormalities. It is sensible to expect that $\alpha > 0.5 > \beta$.

TABLE 1. List of parameters in alphabetical order.

Symbols	Meaning
α	Probability of detection (true positive)
β	Probability of false alarm (false positive)
μ	Prior probability of node being malicious
λ	Probability of a remaining node stays in the neighborhood
b	Benefit of correct strategy
$-b$	Punishment of incorrect strategy
c_a	Cost of attack
c_{gb}	Cost of group for incorrect identification of benign target node
c_{gm}	Cost of group for incorrect identification of malicious target node
c_m	Cost of monitoring of an asset
c_v	Cost of voting
n	Total number of nodes
n_l	Number of nodes left at k^{th} stage
n_r	Number of required votes at k^{th} stage to identify target node
n_{th}	Number of required votes to identify target node
n_{v1}	Number of correct votes for target node
n_{v2}	Number of incorrect votes for target node
p_k	Probability of successful target identification at k^{th} stage
P_m	Probability of monitoring
q	Probability of attack for malicious PLT
s	Probability of voting for monitoring PLB
w	Value of an asset

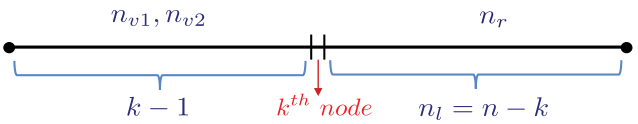

FIGURE 2. k^{th} stage of the game, where n_{v1}, n_{v2}, and n_r denote the number of correct, incorrect, and remaining votes, respectively, and n_l refers to the total number of nodes left to vote.

It is assumed that n nodes are in a neighboring area. Each benign node can vote by paying c_v as the cost of voting. The benefit of a correct strategy and the punishment of an incorrect strategy for a benign node are denoted by b and $-b$, respectively. To generalize the analysis, we design the game at one stage, say the k^{th} stage, in which the type of a target node has not yet been determined. Until this stage, it can be assumed that n_{v1} votes in one type (e.g. malicious) and n_{v2} votes in another type (e.g. benign) have already been cast for the type of target node. We let n_r denote the number of remaining votes required to identify the target node. Therefore, $n_r = n_{th} - n_{v1}$ or $n_r = n_{th} - n_{v2}$, depending on the belief of the k^{th} node on the type of target node. Also, there are n_l nodes left in the game. Fig. 2 helps us understand these parameters. We use p_k to denote the probability of correct target node identification at the k^{th} stage. It is assumed that the cost of the group (neighboring nodes) for the incorrect identification of a malicious target node and a benign target node are c_{gm} and c_{gb}, respectively.

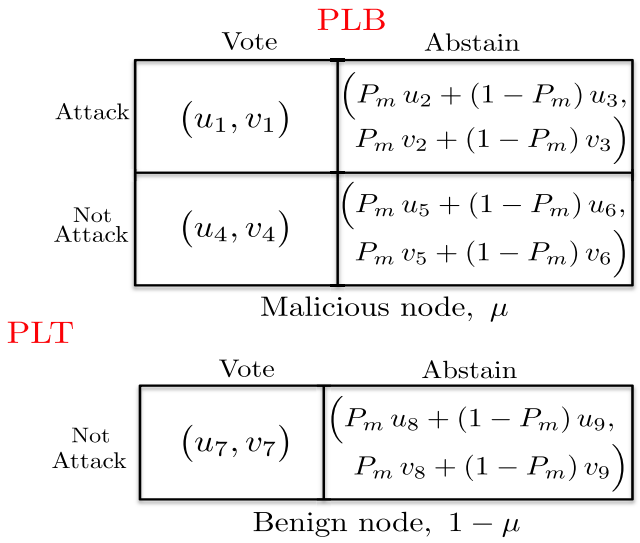

FIGURE 3. Players' payoffs in the game relative to a benign player (PLB) and malicious or benign target node (PLT).

A malicious node can choose to either attack or not attack a benign node based on its information in the game. In this regard, the probability of attack is considered and it is denoted by q in the analysis. Likewise, a node can choose to either vote or not vote. This is captured by defining the probability of voting and is denoted by s in the analysis. It is worth noting that a node considers different parameters to select its strategy, including the accuracy of the monitoring system, costs, benefits, punishments, and the probabilities introduced here. Equipped with these parameters, we are able to design the expected payoffs for players in the game.

B. GAME DEFINITION AND NOTATIONS

Here, we provide some definitions in order to facilitate the description of our model.

Definition 1: A Bayesian game G is defined by a tuple (N, A, Θ, μ, U), where N is a set of players, A is a set of actions, Θ is a set of players' types, μ is a common prior, and U is a set of utilities. These are defined as follows:

- N = (PLT, PLB), where PLT is a target node and PLB is a benign player.
- $A = (a_{PLT}, a_{PLB})$, where $a_{PLT} \in \{\text{attack, not attack}\}$, and $a_{PLB} \in \{\text{vote, abstain}\}$.
- $\Theta = (\theta_{PLT}, \theta_{PLB})$, where $\theta_{PLT} \in \{\text{malicious, benign}\}$, and $\theta_{PLB} \in \{\text{benign}\}$.
- Prior belief: PLB assigns μ for PLT being malicious, and PLB's type is common knowledge.
- $U = (u,\ v)$, where u refers to PLB's payoff, and v refers to PLT's payoff.

Fig. 3 shows the strategic form of the game G, where rows and columns indicate the actions of a target node and a benign player, respectively. As can be seen, each window includes pairs of payoffs (u_z, v_z), where $1 \leq z \leq 9$, and the subscript z refers to the actions of both PLB and PLT in one scenario. For example, (u_1, v_1) at top left window in Fig. 3 corresponds to voting PLB and attacking PLT. As can be seen in Fig. 3, we need to define u_z and v_z to provide the layout of the game.

Definition 2: Each player's payoff can be defined as the summation of an individual payoff and a group payoff as follows:

$$u_z = u_{z,i} + u_{z,g}, \tag{1}$$
$$v_z = v_{z,i} + v_{z,g}, \tag{2}$$

where $u_{z,i}$ and $v_{z,i}$ denote individual payoffs, and $u_{z,g}$ and $v_{z,g}$ denote group payoffs. The individual payoff only considers interactions between two players, while the group payoff accounts for the impact of a player's strategy on all members in the neighborhood.

It is worth noting that the group payoffs capture the impact of a node's strategy on the security of all nodes in the network. This comes from a node by either voting or abstaining in the voting game. Group payoff also provides a framework to capture incentives for promoting cooperation in the game. In particular, the collaboration of nodes for malicious node identification would reward them, while abstaining from the collaboration could punish them in the game. These rewards and penalties are included in the group payoff of a node, because they relate to actions that impact all nodes in the network. The following section describes the design of both individual and group payoffs in detail.

C. PAYOFF DESIGN

In what follows, we describe individual payoffs and group payoffs and find all u_z and v_z shown in Fig. 3. Individual payoffs account for the costs and benefit of monitoring and non-monitoring, whereas group payoffs account for the costs and benefits of voting or abstaining from the game. The incentives of the game, including benefits and punishments, are considered in the group payoffs. This means that a node measures its group payoff before choosing its strategy. Initially, we focus on obtaining individual payoffs, i.e., $u_{z,i}$. Then, we explain group payoffs, i.e., $u_{z,g}$. Finally, we use definition 2 to add individual and group payoffs to obtain all u_z and v_z.

1) INDIVIDUAL PAYOFFS

To study individual interactions between two nodes, note that a malicious node could choose either to attack or not to attack a benign node. Also, the benign node could be either in a monitoring state or a non-monitoring state. Hence, we have four possible scenarios between a malicious node and a benign node:

- A monitoring PLB faces an attacking PLT.
- A non-monitoring PLB faces an attacking PLT.
- A monitoring PLB faces a non-attacking PLT.
- A non-monitoring PLB faces a non-attacking PLT.

What follows is a study of the payoffs for these scenarios to evaluate related $u_{z,i}$ and $v_{z,i}$.

Scenario I: A monitoring PLB faces an attacking PLT. Here, the monitoring PLB pays $-c_m$ as the cost of monitoring.

However, it gains $(2\alpha - 1)w$ from its detection system. This is because the expected gain of the PLB relates to the true positive rate (α) and the false negative rate ($1 - \alpha$) of its detection system, i.e., $\alpha w - (1-\alpha)w$. Therefore, the individual payoff of a monitoring PLB in this scenario is equal to $-c_m + (2\alpha - 1)w$. This payoff corresponds to $u_{1,i}$ and $u_{2,i}$, where the PLT attacks a monitoring PLB. Hence,

$$u_{1,i} = u_{2,i} = -c_m + (2\alpha - 1)w. \tag{3}$$

On the other hand, the PLT pays $-c_a$ as the cost of the attack. The loss of the PLT can be assumed as the negative gain of the PLB's individual payoff [11], i.e. $-(2\alpha - 1)w$. Therefore, the individual payoff for an attacking malicious PLT in this scenario equals $-c_a - (2\alpha - 1)w$. This payoff corresponds to $v_{1,i}$ and $v_{2,i}$. Hence,

$$v_{1,i} = v_{2,i} = -c_a - (2\alpha - 1)w. \tag{4}$$

Scenario II: A non-monitoring PLB faces an attacking PLT. Here, the non-monitoring PLB does not pay the cost of monitoring but loses its asset as a result of being in a non-monitoring state and attacking the PLT. Therefore, the individual payoff of a non-monitoring PLB in this scenario is equal to $-w$. This payoff corresponds to $u_{3,i}$. Hence,

$$u_{3,i} = -w \tag{5}$$

On the other hand, the PLT pays $-c_a$ as the cost of the attack, and its gain is equal to the loss of the non-monitoring PLB, i.e. $+w$. Therefore, the individual payoff for an attacking malicious PLT in this scenario equals $-c_a + w$. This payoff corresponds to $v_{3,i}$. Hence,

$$v_{3,i} = -c_a + w. \tag{6}$$

Scenario III: A monitoring PLB faces a non-attacking PLT. Here, a monitoring PLB pays $-c_m$ as the cost of monitoring. However, since the PLT is in a non-attacking state, any possible detection comes from its false alarm rate, i.e., $-\beta w$. Therefore, the individual payoff of a monitoring PLB in this scenario is equal to $-c_m - \beta w$. This payoff corresponds to $u_{4,i}$, $u_{5,i}$, $u_{7,i}$, and $u_{8,i}$. Hence,

$$u_{4,i} = u_{5,i} = u_{7,i} = u_{8,i} = -c_m - \beta w. \tag{7}$$

The non-attacking PLT does not gain or lose in the interaction. Thus,

$$v_{4,i} = v_{5,i} = v_{7,i} = v_{8,i} = 0. \tag{8}$$

Scenario IV: A non-monitoring PLB faces a non-attacking PLT. Here, since there has been neither an attack from the PLT nor monitoring from the PLB, we have 0 payoff. This payoff corresponds to $u_{6,i}$, $u_{9,i}$, $v_{6,i}$, and $v_{9,i}$. Hence,

$$u_{6,i} = v_{6,i} = u_{9,i} = v_{9,i} = 0. \tag{9}$$

Having $u_{z,i}$ and $v_{z,i}$ in hand, we continue defining $u_{z,g}$ and $v_{z,g}$ to be able to use definition 2 and obtain all payoffs.

2) GROUP PAYOFFS

To study group payoffs, note that a monitoring PLB can choose between voting and abstaining on the type of PLT in the game. A non-monitoring PLB always chooses to abstain from voting because it does not have any information about PLT. In this respect, we can study group payoffs by considering four scenarios:

- Monitoring PLB faces an attacking malicious PLT.
- Monitoring PLB faces a non-attacking malicious PLT.
- Monitoring PLB faces a (non-attacking) benign PLT.
- PLB is in a non-monitoring state.

In the first three scenarios, we study the voting and abstaining strategies of a monitoring PLB w.r.t. the probability of correct target node identification (p_k) in the game. This is because the target node is not yet identified in the network; hence, the PLB should consider the probability of correct, wrong, or undecided target node identification before choosing its strategy. In this regard, we use Fig. 4(a) to show the dependency between a monitoring PLB's strategy and p_k. As shown, the left column corresponds to the player's voting strategy and the right column corresponds to its abstaining strategy. Also, the top row (labeled p_k) refers to the case that the target node is correctly identified in the game, and the lower row (labeled $1 - p_k$) refers to the case that the target node is not correctly identified in the game. In this figure, X, Y, Z, and W denote payoffs for different possible cases. For example, X in the top left window in Fig. 4(a) represents the case where the PLB votes and target node is correctly identified in the game. We will design X, Y, Z, and W for different scenarios between the PLT and a monitoring PLB. Using Fig. 4(a), we define group payoffs for the voting and abstaining strategies of the PLB.

Definition 3: Considering two possible outcomes for target node identification, denoted by p_k and $1 - p_k$ in Fig. 4(a), we define two group payoffs for possible strategies of a monitoring PLB at the k^{th} stage:

$$u_g\,(vote) = p_k\,(X) + (1 - p_k)(Z), \tag{10}$$

$$u_g\,(abstain) = p_k\,(Y) + (1 - p_k)(W), \tag{11}$$

where the payoff of each strategy is weighted by the corresponding probabilities.

In the last scenario, since a non-monitoring PLB always abstains from voting regardless of the PLT's strategy, its group payoff depends on other nodes' actions in the game. In what follows, we study payoffs for all the above scenarios to evaluate related $u_{z,g}$ and $v_{z,g}$.

As can be seen by Eqs. (10)-(11), p_k plays an important role in the payoffs. In this respect, we obtain p_k to evaluate the voting and abstaining strategies of players. It is noteworthy that the value of p_k increases when the PLB votes correctly. We use δ to denote this improvement in p_k.

Lemma 1: p_k and δ can be written as follows:

$$p_k = \sum_{i=n_r}^{n_l} \binom{n_l}{i} (p_s)^i \left(1 - p_s\right)^{n_l - i}, \tag{12}$$

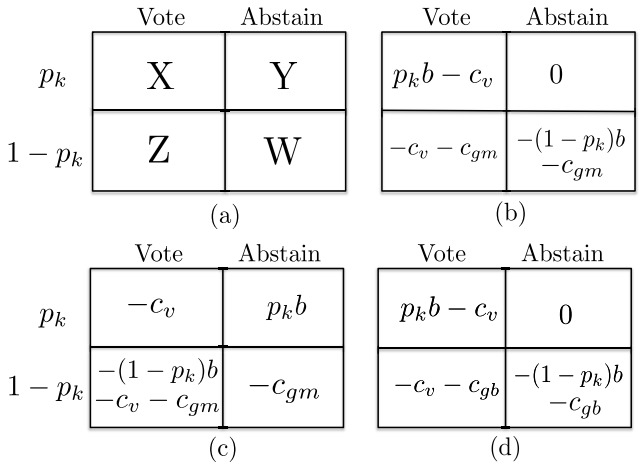

FIGURE 4. Group payoffs: (a) for a monitoring benign player in general, which is then broken down to the following scenarios: (b) malicious target node has attacked a monitoring benign node, (c) malicious target node has not attacked a monitoring benign node, and (d) benign target node versus a monitoring benign node.

$$\delta = \binom{n_l}{n_r - 1} (p_s)^{n_r - 1} (1 - p_s)^{n_l - (n_r - 1)}, \quad (13)$$

where $p_s \triangleq \lambda(1-\mu)\alpha P_m$ *represents the probability of correct target identification by a remaining node in the game.*

This lemma and theorems are proved in the appendix.

Scenario I: The monitoring PLB faces the attacking malicious PLT, which relates to the first row of Fig. 3. The group payoffs in this scenario correspond to $u_{1,g}$, $u_{2,g}$, $v_{1,g}$, and $v_{2,g}$. Fig. 4(b) shows the voting payoff (i.e., $u_{1,g}$) and the abstaining payoff (i.e., $u_{2,g}$) for a monitoring PLB w.r.t. p_k. As can be seen in Fig. 4(b), $-c_v$ in the left column (i.e., vote) represents the cost of voting. Also, $-c_{gm}$ in the lower row (i.e., $1 - p_k$) denotes the cost of incorrect identification for a malicious target node. The reward for voting in correct target identification (top left window) and the punishment of abstaining in incorrect target identification (bottom right window) are represented by bp_k and $-b(1-p_k)$, respectively. These are proportional to p_k because the player's expected outcome is entangled with the probability of correct target node identification (p_k) in the middle of the game. The reward and the punishment are considered (as incentives) to encourage nodes in cooperation. Using Fig. 4(b) along with equations (10) and (11) in definition 3, we have

$$\begin{aligned} u_{1,g} &= p_k \times \big(p_k b - c_v\big) + \big(1 - p_k\big) \times \big(-c_v - c_{gm}\big), \\ \Rightarrow u_{1,g} &= p_k^2 b - c_v - (1 - p_k)c_{gm}, \quad (14) \\ u_{2,g} &= p_k \times \big(0\big) + \big(1 - p_k\big) \times \big(-(1 - p_k)b - c_{gm}\big), \\ \Rightarrow u_{2,g} &= -(1 - p_k)^2 b - (1 - p_k)c_{gm}. \quad (15) \end{aligned}$$

We also define group payoffs for the PLT in this scenario by $(1 - p_k)c_{gm}$, which indicates the inverse proportional relationship between p_k and the gain of the malicious PLT. Hence, we have

$$v_{1,g} = v_{2,g} = (1 - p_k)c_{gm}. \quad (16)$$

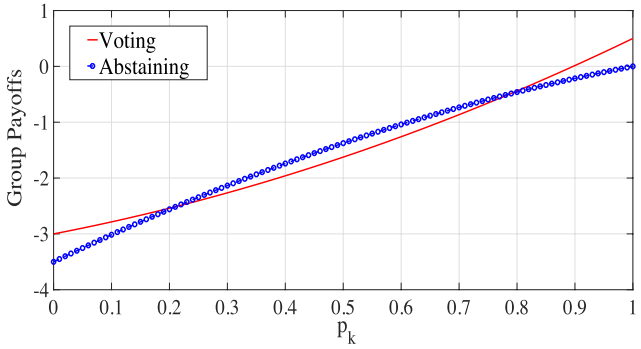

FIGURE 5. Group payoffs for monitoring benign node relative to p_k.

In order to better understand the impact of a node's group payoff on selecting its strategy, we provide a plot in Fig. 5 that shows voting payoffs (i.e., $u_{1,g}$) and abstaining payoffs (i.e., $u_{2,g}$) of PLB w.r.t. different p_ks in this scenario. Here, it is assumed that $c_v = 1$, $b = 1.5$, and $c_{gm} = 2$. As can be seen, depending on the value of p_k, voting payoffs can outweigh abstaining payoffs, and vice versa. For example, voting payoffs are dominant for $p_k < 0.2$, which means that the player votes in this interval of p_k. In fact, voting is an attempt by PLB to increase p_k and avoid an incorrect outcome of the game. The main motivation of the player, however, comes from the game's punishment. That is, the cost of voting is lower than the punishment of the game when the malicious target node is not correctly identified. In other words, if $p_k \to 0$, then $-c_v > -(1 - p_k)b$ (see lower row of Fig. 4(a)). Therefore, the player votes not only to increase p_k but also to avoid punishment in the game. The same reasoning can be used for other intervals of p_k, i.e., $p_k > 0.8$ and $0.2 < p_k < 0.8$, to determine the motivations of the player for voting and abstaining in the game.

Scenario II: The monitoring PLB faces the non-attacking malicious PLT, which relates to the second row of Fig. 3. The group payoffs in this scenario correspond to $u_{4,g}$, $u_{5,g}$, $v_{4,g}$, and $v_{5,g}$. Fig. 4(c) shows the voting payoff (i.e., $u_{4,g}$) and the abstaining payoff (i.e., $u_{5,g}$) for a monitoring PLB w.r.t. p_k. Here, a monitoring PLB might unintentionally support a malicious PLT by its vote because the malicious PLT is in a non-attacking state. In this regard, we define a penalty by $-(1 - p_k)b$ for voting in an incorrect target identification (bottom left window), and a reward by $p_k b$ for abstaining in a correct target identification (top right window). This prevents the PLB from blind voting (solely to gain the benefit of collaboration) when it did not sense abnormalities from a node. Using Fig. 4(c) along with equations (10) and (11) in definition 3, we have

$$\begin{aligned} u_{4,g} &= p_k\big(-c_v\big) + \big(1 - p_k\big)\big(-(1 - p_k)b - c_v - c_{gm}\big), \\ \Rightarrow u_{4,g} &= -(1 - p_k)^2 b - c_v - (1 - p_k)c_{gm}, \quad (17) \\ u_{5,g} &= p_k \times \big(p_k b\big) + \big(1 - p_k\big) \times \big(-c_{gm}\big), \\ \Rightarrow u_{5,g} &= p_k^2 b - (1 - p_k)c_{gm}. \quad (18) \end{aligned}$$

Since the malicious PLT is in a non-attacking mode, we define $v_{4,g} = v_{5,g} = 0$, which implies that the non-attacking PLT does not gain or lose in this scenario.

Scenario III: The monitoring PLB faces a (non-attacking) benign PLT, which relates to the third row of Fig. 3. The group payoffs in this scenario correspond to $u_{7,g}$, $u_{8,g}$, $v_{7,g}$, and $v_{8,g}$. Fig. 4(d) shows the voting payoff (i.e., $u_{7,g}$) and the abstaining payoff (i.e., $u_{8,g}$) for a monitoring PLB w.r.t. p_k. The design of payoffs in Fig. 4(d) is quite similar to scenario I in Fig. 4(b), where c_{gm} is replaced by c_{gb}. Hence, the reasoning for this scenario follows the same lines as scenario I. Using Fig. 4(c) along with equations (10) and (11) in definition 3, we have

$$\begin{aligned} u_{7,g} &= p_k \times \big(p_k b - c_v\big) + \big(1-p_k\big) \times \big(-c_v - c_{gb}\big), \\ \Rightarrow u_{7,g} &= p_k^2 b - c_v - (1-p_k)c_{gb}, \end{aligned} \tag{19}$$

$$\begin{aligned} u_{8,g} &= p_k \times \big(0\big) + \big(1-p_k\big) \times \big(-(1-p_k)b - c_{gb}\big), \\ \Rightarrow u_{8,g} &= -(1-p_k)^2 b - (1-p_k)c_{gb}. \end{aligned} \tag{20}$$

Since benign PLT is in a non-attacking mode, we have $v_{7,g} = v_{8,g} = 0$.

Scenario IV: The PLB is in a non-monitoring state. In this case, the PLB abstains from voting, regardless of the PLT's strategy. The group payoffs in this scenario correspond to $u_{3,g}$, $u_{6,g}$, $u_{9,g}$, $v_{3,g}$, $v_{6,g}$, and $v_{9,g}$. To define $u_{3,g}$ and $u_{6,g}$, where the PLT is malicious, we know that the non-monitoring PLB completely relies on other nodes for target node identification. If $p_k = 1$, then the node is not harmed, but if $p_k = 0$, then it gets $-c_{gm}$ as the cost of the incorrect malicious PLT identification. Thus, we define $u_{3,g} = u_{6,g} = -(1-p_k)c_{gm}$, where the node does not impact the group decision while it is affected by other decisions. We can apply a similar reasoning for $u_{9,g}$, with the only difference being that c_{gm} is replaced by c_{gb}, because the PLT is benign, i.e., $u_{9,g} = -(1-p_k)c_{gb}$. On the other hand, we define $v_{3,g} = (1-p_k)c_{gm}$, which reflects the inverse proportional relationship between p_k and the gain of the attacking malicious PLT. In the case of $v_{6,g}$ and $v_{9,g}$, the benign PLT does not attack; hence, there is no gain or loss, i.e., $v_{6,g} = v_{9,g} = 0$.

3) TOTAL PAYOFFS

By designing individual payoffs and group payoffs for each scenario in the game, we can use definition 2 to obtain all payoffs. For example, u_1 is the summation of $u_{1,i}$ (i.e., equation (3)) and $u_{1,g}$ (i.e., equation (14)). Thus, using equation (1) in definition 2, we have

$$u_1 = -c_m + (2\alpha - 1)w + p_k^2 b - c_v - (1-p_k)c_{gm}, \tag{21}$$

We obtain the remaining payoffs in the same fashion, as follows:

$$u_2 = -c_m + (2\alpha - 1)w - (1-p_k)^2 b - (1-p_k)c_{gm}, \tag{22}$$

$$u_3 = -w - (1-p_k)c_{gm}, \tag{23}$$

$$u_4 = -c_m - \beta w - (1-p_k)^2 b - c_v - (1-p_k)c_{gm}, \tag{24}$$

$$u_5 = -c_m - \beta w + p_k^2 b - (1-p_k)c_{gm}, \tag{25}$$

$$u_6 = -(1-p_k)c_{gm}, \tag{26}$$

$$u_7 = -c_m - \beta w + p_k^2 b - c_v - (1-p_k)c_{gb}, \tag{27}$$

$$u_8 = -(1-p_k)^2 b - (1-p_k)c_{gb} - c_m - \beta w, \tag{28}$$

$$u_9 = -(1-p_k)c_{gb}, \tag{29}$$

$$v_1 = v_2 = -c_a - (2\alpha - 1)w + (1-p_k)c_{gm}, \tag{30}$$

$$v_3 = -c_a + w + (1-p_k)c_{gm}, \tag{31}$$

$$v_4 = v_5 = v_6 = v_7 = v_8 = v_9 = 0. \tag{32}$$

D. VARIABLE-BENEFIT SCHEME

So far, we have assumed that the benefit of a correct strategy (b) is constant, irrespective of its impact on the outcome of the game. In principle, a variable benefit could be designed to be commensurate with the impact of k^{th} player's strategy on the target node identification. In this regard, we choose p_k and μ as two important arguments that directly affect the value of a strategy in the game. We categorize these benefits into two cases. The first is the benefit when the PLB has detected an abnormality in the PLT. This implies that the malicious PLT has attacked the PLB, or that the abnormality simply comes from a false alarm. We denote the benefit for a correct strategy in this case by b_1. Here, group payoffs are the same as in Fig. 4(a), wherein $b = b_1$. The second case is when a monitoring PLB has not detected any abnormalities from the PLT, i.e., whether the PLT is malicious or benign. We denote the benefit for a correct strategy in this case by b_2. Payoff tables for this case are the same as those in Fig. 4(b) and Fig. 4(c), wherein $b = b_2$. By making the PLB indifferent, b_1 and b_2 can be derived.

Lemma 2: b_1 and b_2 for the k^{th} stage of the game can be obtained as follows:

$$b_1 = \frac{c_v}{(2p_k^2 - 2p_k + 1)}, \tag{33}$$

$$b_2 = \frac{c_v}{(1-2\mu)(2p_k^2 - 2p_k + 1)}. \tag{34}$$

Assuming $c_v = 1$, the value of b_1 and b_2 versus p_k and μ are shown in Fig. 6. As can be seen in Fig. 6(a), when $p_k = 0.5$, the highest b_1 occurs, and when $p_k = 0$ or $p_k = 1$, the lowest b_1 occurs, underlining the fact that the highest benefit is rewarded for a PLB that faces the highest uncertainty of p_k (similar to gambling!). On the other hand, as shown in Fig. 6(b), when μ (the portion of malicious nodes) grows, the value of benefits also increases. This is not surprising because as μ increases, benign nodes should be more motivated for participation to reveal the identity of a target node before malicious nodes determine the game's result with their votes.

Here, we study the impact of b_1 on group payoffs. The study of group payoffs with b_2 can be done in the same fashion. Fig. 7 shows group payoffs with $b = b_1$, where each subplot corresponds to a window in Fig. 4(b). For example, the top left subplot in Fig. 7 refers to $p_k b - c_v$ in Fig. 4(b), where $b = b_1$. In Fig. 7, we assume that $c_v = 1$ and $c_{gm} = 4$. As can be seen, payoffs in the upper row dominate over those in the lower row. This is because the upper payoffs

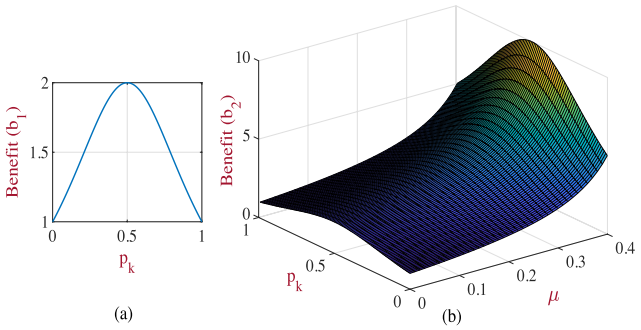

FIGURE 6. Benefits with regard to probability of successful target identification in k^{th} stage (p_k) and portion of malicious nodes (μ) in network.

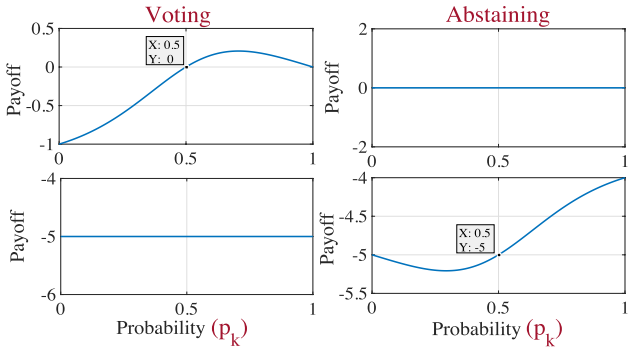

FIGURE 7. Expected group payoffs for scenario I with variable benefits.

show successful target node identification, while the lower payoffs indicate the unsuccessful counterpart. To understand this better, let us study the trend of graphs for a few p_ks. First, let $p_k = 0.25$, which yields $b_1 = 1.6$ from eq. (33). Under this assumption, if the game is to successfully identify the target node (upper row in Fig. 7), then PL2 collects a higher payoff by abstaining ($0 > -0.6$). However, if the game becomes unsuccessful (lower row), then PL2 should have voted in the game ($-5 > -5.2$). Next, assume that $p_k = 0.75$. Interestingly, we obtain the same benefit (i.e., $b_1 = 1.6$). In this case, however, the strategy of PL2 will be the opposite. That is, PL2 is willing to vote if it thinks the game will be successful ($0.2 > 0$), while it abstains if it thinks the game will be unsuccessful ($-.4.4 > -5$). This example helps us summarize the following intuitions for the case of adaptive benefit: (i) There is no pure strategy for PL2 during the game w.r.t. a specific p_k or b; and (ii) $p_k = 0.5$ is the only point where PL2 becomes completely indifferent between voting and abstaining, regardless of the result of the game (see $p_k = 0.5$ in Fig. 7). This is the place where our design offers the highest benefit (see Fig. 6) in order to encourage PL2 to participate, hence, increase p_k.

IV. EQUILIBRIUM ANALYSIS

The objective of the players is to maximize their payoffs in the game. In this regard, we obtain possible equilibrium points using a Bayesian game to better understand the behavior of the players. In particular, we obtain the best strategies of benign players to identify a malicious node, while we find the maximum level of aggressiveness for malicious nodes without being identified. In this respect, we use the interactions between a PLB and a PLT, as illustrated in Fig. 3. Let us quickly summarize the possible strategies of the players. A non-monitoring PLB has one pure strategy: abstaining. A monitoring PLB has two strategies: voting or abstaining. A benign PLT has one pure strategy: to not attack. Finally, a malicious PLT could choose two strategies: to attack or not to attack. Depending on game parameters, a pure-strategy BNE may or may not exist. This is addressed in the following theorem.

Theorem 1: Given μ and P_m, if $c_{gm} \geq c_a + (2\alpha - 1)\, w + \delta c_{gm}$, and $b > 2\, c_v$, then the game has one pure-strategy BNE. A malicious node attacks and a monitoring benign node votes in the game.

Remark 1: When the damage caused by incorrect malicious node identification (c_{gm}) is higher than the summation of PLT's cost of attack (c_a), PLT's individual loss against a monitoring PLB, i.e., $(2\alpha - 1)\, w$, (see eq. (4)), and the impact of PLB's vote in the game (δc_{gm}), then a malicious node attacks a benign node. When the benefit of voting for a monitoring PLB is more than twice of its cost, then the benign node chooses to vote.

The pure-strategy BNE, as seen above, holds only under certain conditions on the parameters. Our game is a finite strategic-form game. Hence, a mixed-strategy BNE can be applied to gain a broader perspective for the game analysis. In this regard, to determine each player's indifference strategy, we define q as the probability of attack for a malicious PLT, and s as the probability of voting for a monitoring PLB.

Theorem 2: Given μ and P_m, the game defined in section III has a mixed-strategy BNE, which is as follows:

- Malicious node attacks with a probability of q^*, which is

$$q^* = \frac{q_1 + q_2 + \cdots + q_n}{n}, \tag{35}$$

where q_k, $k = 1, \ldots, n$, is the probability of attack for the k_{th} node in the game

$$\begin{aligned} q_k &= \frac{A_k}{B_k}, \\ A_k &= \mu\big(1 + P_m\big)\big(2p_k^2 - 2p_k + 1\big)b + \big(1 - P_m\big) \\ &\quad \times \big(c_m + \beta w\big) + c_v - p_k^2 b - P_m\big(1 - p_k\big)^2 b, \\ B_k &= \mu\big(1 + P_m\big)\big(2p_k^2 - 2p_k + 1\big)b \\ &\quad + \mu\big(1 - P_m\big)(2\alpha + \beta)w. \end{aligned} \tag{36}$$

- Monitoring benign node votes with probability of s^*, which is equal to

$$s^* = \frac{c_a + (2\alpha P_m - 1)w - c_{gm}}{(1 - P_m)[-c_a + (1 - 2\alpha)w + c_{gm}] - \delta c_{gm}}. \tag{37}$$

Note that the mixed-strategy provides general equilibrium points w.r.t. different parameters. In a special case, if all nodes monitor their neighbors, i.e., $P_m = 1$, then an upper bound

for the benefit and a lower bound for the detection rate can be derived using eqs. (36) and (37), respectively.

Corollary 1: In Theorem 2, if $P_m = 1$, then

$$b < \frac{c_v}{(1-2\mu)(2p_k^2 - 2p_k + 1)}, \tag{38}$$

$$\alpha > \frac{w - c_a + c_{gm}(1-\delta)}{2w}. \tag{39}$$

From eq. (38), it can be seen that as $\mu \to \frac{1}{2}$, the upper bound increases. This allows network designers to select higher values of benefit in environments where the probability of a malicious PLT is higher. On the other hand, eq. (39) implies that a monitoring system must have a minimum true positive rate in order to make a malicious node indifferent in the game.

Corollary 2: In Theorem 2, if $P_m = 1$, and benefits are designed using b_1 and b_2 in Eqs. (33) and (34), then the probability of attack by a malicious node will be zero, i.e., $q^* = 0$.

While the result of this corollary is the most desirable outcome for every game designer, we should note that achieving it might require a strong assumption ($P_m = 1$) and a complex system for a beneficial design, because it requires all monitoring nodes in an ephemeral network that adapt their benefits in each stage according to p_k.

In the next section, we evaluate the performance of the game in order to obtain a better picture of the above analysis.

V. NUMERICAL RESULTS

To evaluate our analysis, we assume that 40 nodes can run the game in an area that is 625 m × 625 m (normal density $\approx 100 \frac{\text{nodes}}{km^2}$ in [33]). Since the analysis is probabilistic, we run 100 iterations for each simulation. Then, we take an average of the results with 95% confidence interval. The default game parameters are as follows:

- Monitoring system parameters: $\alpha = 0.95$, $\beta = 0.05$,
- Probabilities: $P_m = 0.75$, $\mu = 0.2$, and $q = 0.4$,
- Costs and benefits: $c_{gb} = c_{gm} = 4$, $w = 4$, $b = 3$, $c_m = c_a = c_v = 1$.

If we change these parameters to better explain a scenario, then we will explicitly mention it. Nevertheless, we describe the theoretical results in three subsections. Initially, we study the impact of incentives (in particular, b) on correct, wrong, and undecided target node identification. Then, we focus on the behavior of malicious nodes w.r.t. their portion and aggressiveness in the network. This section also includes a comparison among different n_{th}s. Finally, we compare our work with scenarios where the uncertainties discussed in this paper have not been considered, e.g., [15], [17], [20]. In all these cases, we evaluate and compare the percentage of target node identification for different sets of given parameters that lead to different equilibria for the game.

A. IMPACT OF INCENTIVES

Fig. 8 illustrates the percentage of target node identification versus b. Here, it is assumed that $q = 0.7$. As shown,

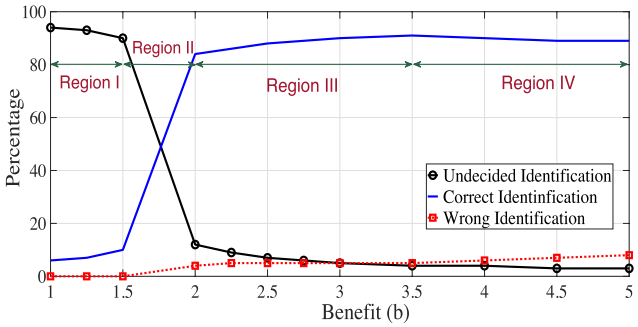

FIGURE 8. Game outcomes versus benefit variations.

this figure can be categorized into four different regions. In region I, the percentage of undecided target identification outweighs correct and wrong identifications for a simple reason: the benefit is not large enough to persuade nodes to participate in the game. Region II, however, illustrates a drastic reduction of undecided identification. This indicates that voting payoffs become larger in comparison to abstaining payoffs. In addition, correct identification dominates over wrong identification, which is the result of the following: (i) benign nodes with high monitoring and detection rates (i.e., $P_m = 0.75$ and $\alpha = 0.95$), and (ii) malicious nodes with a high level of aggressiveness (i.e., $q = 0.7$). Region III shows a slight increase in correct identification and a decrease in undecided identification because of lower payoffs for abstaining from the game. The increase of wrong identification over undecided identification is remarkable in region IV. Wrong votes in this region mainly come from highly encouraged benign nodes that have not been attacked by a malicious target node. In other words, since voting payoffs are significantly larger than abstaining payoffs (i.e., $u_4 > u_5$ and $u_7 > u_8$), a benign node votes in favor of a non-attacking target node. This observation reveals that persuading every node to vote by applying the leverage of benefit does not necessarily lead to a better outcome. Taking all regions into consideration, region III indicates the best option for the benefit design.

B. IMPACT OF MALICIOUS NODES AND N_{TH}

Fig. 9 shows the percentage of target identification w.r.t. the portion of malicious nodes and their probability of attack (q) in the network. As shown, when q increases, correct identification generally increases, which confirms that aggressive attackers can be more easily identified. However, wrong identification is reduced after a certain value of q; for example, $q = 0.1$ for $\mu = 0.1$. When the number of malicious nodes increases in the network, this decreasing trend starts at higher values of q; for instance, $q = 0.4$ for $\mu = 0.2$. This reveals that malicious nodes become more aggressive when their number increases in the network.

Fig. 10 depicts identification results w.r.t. the variation of n_{th} and μ. As n_{th} grows larger, a turning point occurs, whereby undecided identification prevails over correct and wrong identifications. The reason is that a higher number of nodes must participate to make an outcome of identification.

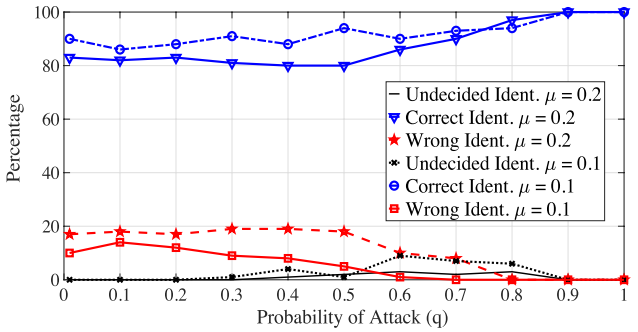

FIGURE 9. Impact of portion of malicious nodes (μ) and probability of attack (q) on identification results.

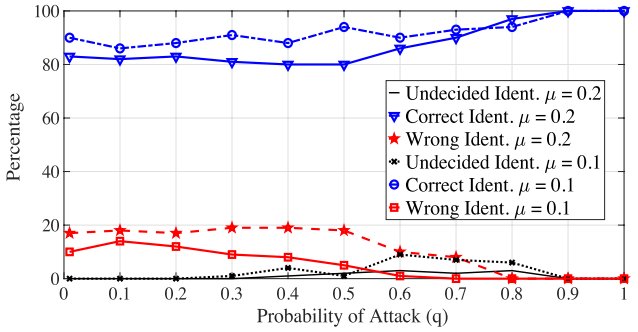

FIGURE 10. Impact of required votes, n_{th}, on target identification.

For example, consider plots for $\mu = 0.2$, where $n_{th} = 23$ is the turning point. This number comes from the fact that out of 40 neighboring nodes, on average, 8 of them are malicious nodes (40×0.2). Also, from the remaining 32 benign nodes, those that are in the monitoring state, i.e., 24 (32×0.75), might vote depending on their payoffs. If $n_{th} = 23$, then almost all such nodes must participate to avoid undecided target identification. A designer can adjust the n_{th} w.r.t. a range of μs to obtain an acceptable correct identification rate.

C. COMPARISON

In this section, we compare our work with the scenarios where some of the explained uncertainties have not been considered (e.g. [15], [17], [20]). It is worth mentioning that the comparison is limited to highlighting uncertainties in those scenarios. This is because the nature of their games and objectives are slightly different. However, this comparison provides us with insight into the effect of incomplete information at nodes on the outcome of a local voting game.

Fig. 11(a) shows the impact of the true positive detection rate (α) on the correct target identification. As can be seen, it is essential for nodes to have high values of α in order to gain high correct target identification. The values of α become more important when fewer benign nodes monitor their neighbors (i.e., smaller P_m). Fig. 11(b) indicates a comparison between a design with and without uncertainties in the local voting game. In particular, we assume that a design without uncertainty has the following parameters: $\alpha = 1$, $\beta = 0$, and $q = 1$. As shown, the difference between

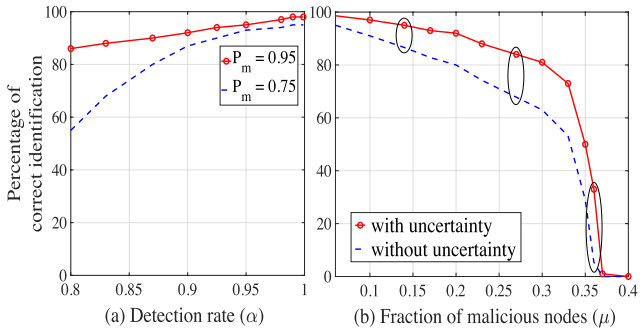

FIGURE 11. Impact of game uncertainties relative: (a) detection rate, and (b) correct identification rate.

graphs is the growth of μ. This is because a player without uncertainty considers a non-attacking malicious node as a benign node and votes for it. On the other hand, the proposed design prevents benign nodes from voting when they are unsure about the strategy of malicious nodes. In both scenarios, when μ goes beyond a threshold, here 0.3, correct target identification is significantly reduced. This comes from higher payoffs for abstaining in comparison to voting. Interpreted differently, benign nodes are unwilling to cooperate in a game in which a high portion of participants are malicious.

VI. CONCLUSION

In this paper, we have provided a game-theoretic approach to identify malicious nodes in ephemeral networks, where central stations are not available. In particular, we have studied the strategies of nodes in a local voting-based game using a Bayesian game, in which nodes have incomplete information about the accuracy of their monitoring systems, the type of neighbors (benign or malicious), and the outcome of the game. By offering incentives in expected utilities, we have provided encouragements for game participation with the aim of improving correct node identification. We have derived possible Bayesian Nash equilibrium (BNE) points and mixed-strategy BNE points to study the best strategies of players in the game. Simulation results have shown the impact of different parameters, such as participation benefits and detection rate, on the identification of malicious nodes.

APPENDIX

A. PROOF OF LEMMA 1

Proof: To obtain p_k, note that n_{v1} and n_{v2} votes have already been cast until the k^{th} stage, while there are n_l nodes left in the game. To derive a closed form for p_k, note the following: (i) If $n_r > n_l$, then $p_k = 0$, which means that the number of left nodes is less than the number of required votes to identify the PLT; (ii) if $n_r = 0$, then $p_k = 1$, which implies that the PLT has been already identified; (iii) p_k directly depends on n_l and their type; and (iv) if n_r is reduced, then p_k will be increased. Taking these points into account, p_k can be written in the form of eq. (12), where p_s represents the probability of correct target node identification. For instance, assume $n = 10$, $k = 7$ (i.e., $n_l = 3$), $p_s = 1/3$, and $n_{th} = 4$.

Under such assumptions, if $n_{v1} = 0$ (i.e., $n_r = 4$), then equation (12) yields $p_k = 0$ because of the first condition. If $n_{v1} = 4$ (i.e., $n_r = 0$), then eq. (12) yields $p_k = 1$ because of the second condition. Also, substituting $n_r = 1$ and $n_r = 3$, respectively, yields $p_k = 0.7$ and $p_k \approx 0.04$, which confirm the last condition. We can define $p_s = \lambda(1-\mu)\alpha P_m$, where λ represents the probability of a remaining node to be in the network and $1-\mu$ is the probability of the remaining node to be benign.

Since δ is defined as the difference that a correct vote can make in p_k, we have

$$\begin{aligned} \delta &= p_k(voting) - p_k(abstaining), \\ \Rightarrow\ \delta &= \sum_{i=n_r-1}^{n_l} \binom{n_l}{i} (p_s)^i (1-p_s)^{n_l-i} \\ &\quad - \sum_{i=n_r}^{n_l} \binom{n_l}{i} (p_s)^i (1-p_s)^{n_l-i}, \end{aligned} \tag{40}$$

which yields eq. (13). □

B. PROOF OF LEMMA 2

Proof: A node must remain indifferent between voting and abstaining for all p_ks and μs. That is,

$$\begin{aligned} Eu(voting)_z &= Eu(abstaining)_z, \\ z &\triangleq \{attack, not\ attack\}, \end{aligned} \tag{41}$$

where $Eu(.)$ denotes expected utility function, and z is the strategy of PLT. Applying eq. (41) for b_1 (Fig. 4(a)), and assuming small values of β, we obtain

$$\begin{aligned} p_k(p_k b_1 - c_v) + (1-p_k)(-c_v - c_{gm}) \\ = (1-p_k)[-(1-p_k)b_1 - c_{gm}]. \end{aligned} \tag{42}$$

Simplifying eq. (42) yields eq. (33). Eq. (34) can be obtained in the same fashion using Figs. 4(b)-(c). □

C. PROOF OF THEOREM 1

Proof: We first derive combined payoffs for two types of PLT (malicious and benign) and the PLB. Then, using strictly dominated strategies, we prove the theorem w.r.t. the conditions.

Fig. 12 shows the combination of payoffs. The first and the second element of each column (e.g., $\{A, NA\}$) indicate the strategy of a malicious PLT and a benign PLT. For instance, $\{A, NA\}$ represents the attacking (A) and the non-attacking (NA) strategies from PLT. In addition, ϕ_is and ν_is denote expected payoffs for the PLT and the PLB, respectively. For instance, ν_1 is obtained as follows:

$$\nu_1 = \mu P_m u_1 + (1-\mu) P_m u_7, \tag{43}$$

where u_1 and u_7 are obtained in eqs. (21) and (27), respectively. Based on the values of ϕ_is, if $c_{gm} \geq c_a + (2\alpha - 1)w + \delta c_{gm}$, then the left column in Fig. 12 ($\{A, NA\}$) strictly dominates the right column ($\{NA, NA\}$). On the other hand,

PLB \ PLT	{A, NA}	{NA, NA}
Vote	$\nu_1,\ \phi_1$	$\nu_2,\ \phi_2$
Abstain	$\nu_3,\ \phi_3$	$\nu_4,\ \phi_4$

FIGURE 12. Expected payoffs for combined types of PLT and the PLB.

we need to show that $\nu_1 > \nu_3$ to obtain pure-strategy BNE. Substituting the equations of ν_1 and ν_3 yields

$$\begin{aligned} &(1-P_m)\mu w + (1-P_m)(1-\mu)(1-p_k)c_{gb} + (1-P_m) \\ &\quad \times \mu(1-p_k)c_{gm} + P_m[(2p_k^2 - 2p_k + 1)\,b - c_v] > 0 \end{aligned} \tag{44}$$

As can be seen, the first three items in eq. (44) are equal to or greater than zero. Hence, it suffices to say that the last term is positive. This happens only if $b > \frac{c_v}{(2p_k^2 - 2p_k + 1)}$. This inequality, however, must hold for all p_ks, which means that the right-hand side of the inequality must be maximized. This yields $p_k = 0.5$, which implies $b > 2\,c_v$. □

D. PROOF OF THEOREM 2

Proof: To obtain q^*, we first equalize the expected utilities for voting and abstaining to obtain q_k. Then, we take an average over all possible values of the p_ks to get eq. (35). In this way

$$Eu\left[voting\right] = Eu\left[abstaining\right] \tag{45}$$

where,

$$Eu\left[voting\right] = \mu q u_1 + \mu(1-q)u_4 + (1-\mu)u_7, \tag{46}$$

$$\begin{aligned} Eu\left[abstaining\right] &= \mu\, q\, P_m u_2 + \mu\, q(1-P_m)u_3 \\ &\quad + \mu\,(1-q)P_m u_5 + \mu(1-q)(1-P_m)u_6 \\ &\quad + (1-\mu)P_m u_8 + (1-\mu)(1-P_m)u_9. \end{aligned} \tag{47}$$

Substituting eqs. (21), (24), and (27) into eq. (46), and eqs. (22), (23), (25), (26), (28), and (29) into eq. (47), and then substituting eqs. (46) and (47) in eq. (45) yields eq. (36). Since the malicious PLT might attack the neighboring nodes regardless of their stage in the game, we take an average over all values of q_ks, which yields eq. (35).

To calculate s^*, we can equalize the expected utilities of attack and not attack from the PLT, hence obtaining

$$\mu\, s\, \nu_1 + P_m\, \mu\, (1-s)\, \nu_2 + (1-P_m)\, \mu\, \nu_3 = 0. \tag{48}$$

Plugging eqs. (30) and (31) back into eq. (48) yields eq. (37). □

ACKNOWLEDGMENT

This work was presented in part at the 2019 Allerton Conference on Communication, Control, and Computing [1].

REFERENCES

[1] A. Behfarnia and A. Eslami, "Local voting games for misbehavior detection in VANETs in presence of uncertainty," in *Proc. 57th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, 2019, pp. 480–486.

[2] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das, "Vehicular social networks: A survey," *Pervasive Mobile Comput.*, vol. 43, pp. 96–113, Jan. 2018.

[3] L. Yin, Y. Guo, F. Li, Y. Sun, J. Qian, and A. Vasilakos, "A game-theoretic approach to advertisement dissemination in ephemeral networks," *World Wide Web*, vol. 21, no. 2, pp. 241–260, 2018.

[4] T. Qiu, B. Chen, A. K. Sangaiah, J. Ma, and R. Huang, "A survey of mobile social networks: Applications, Social Characteristics, and challenges," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3932–3947, Dec. 2018.

[5] E. C. Akrida, L. Gasieniec, G. B. Mertzios, and P. G. Spirakis, "Ephemeral networks with random availability of links: Diameter and connectivity," *J. Parallel Distrib. Comput.*, vol. 87, pp. 109–120, Jun. 2016.

[6] R. Van der Heijden, S. Dietzel, and F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," in *Proc. 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Commun.*, Innsbruck, Austria, 2013, pp. 23–25.

[7] S. Shivshankar and A. Jamalipour, "An evolutionary game theory-based approach to cooperation in VANETs under different network conditions," *IEEE Trans. Veh. Techonol.*, vol. 64, no. 5, pp. 2015–2022, May 2015.

[8] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Misbehavior detection and efficient revocation within VANET," *J. Inf. Secur. Appl.*, vol. 46, pp. 193–209, Jun. 2019.

[9] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 4th Quart., 2018.

[10] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Netw.*, vol. 84, pp. 124–147, Oct. 2019.

[11] Y. Liu, C. Comaniciu, and H. Man, "Modeling misbehavior in ad hoc networks: A game theoretic approach for intrusion detection," *J. Secur. Netw.*, vol. 1, nos. 3–4, pp. 243–254, 2006.

[12] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 1–39, 2013.

[13] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," *J. Parallel Distrib. Comput.*, vol. 75, pp. 184–197, Jan. 2015.

[14] M. Raya, M. H. Manshaei, M. Félegyházi, and J.-P. Hubaux, "Revocation games in ephemeral networks," in *Proc. 15th ACM Conf. Comput. Commun. Secur.*, Alexandria, VA, USA, 2008, 199–210.

[15] I. Bilogrevic, M. H. Manshaei, M. Raya, and J.-P. Hubaux, "Optimal revocations in ephemeral networks: A game-theoretic framework," in *Proc. 8th Int. Symp. Model. Optim. Mobile Ad Hoc Wireless Netw. (WiOpt)*, Avignon, France, 2010, pp. 21–30.

[16] B. Liu, J. T. Chiang, and Y.-C. Hu, "Limits on revocation in VANETs," in *Proc. 8th Int. Conf. Appl. Cryptogr. Netw. Secur.*, Beijing, China, 2010, pp. 38–52.

[17] A. A. A. Abass, N. B. Mandayam, and Z. Gajic, "An evolutionary game model for threat revocation in ephemeral networks," in *Proc. 51st Annu. Conf. Inf. Sci. Syst. (CISS)*, Baltimore, MD, USA, 2017, pp. 1–5.

[18] S. J. I. Lekha and R. Kathiroli, "Trust based certificate revocation of malicious nodes in MANET," in *Proc. Int. Conf. Adv. Commun., Control Comput. Technol.*, Ramanathapuram, India, 2014, pp. 1185–1189.

[19] S. Kim, "Effective certificate revocation scheme based on weighted voting game approach," *IET Inf. Secur.*, vol. 10, no. 4, pp. 180–187, 2016.

[20] M. Masdari, "Towards secure localized certificate revocation in mobile ad-hoc networks," *IETE Tech. Rev.*, vol. 34, no. 5, pp. 561–571, 2017.

[21] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP J. Wireless Commun. Netw.*, 2018, p. 62, Dec. 2018.

[22] I. Diakonikolas and C. Pavlou, "On the complexity of the inverse semi-value problem for weighted voting games," in *Proc. AAAI Conf. Artif. Intell.*, Honolulu, HI, USA, 2019, pp. 1869–1876.

[23] B. Subba, S. Biswas, and S. Karmakar, "Intrusion detection in mobile ad-hoc networks: Bayesian game formulation," *Eng. Sci. Technol., Int. J.*, vol. 19, no. 2, pp. 782–799, Jun. 2016.

[24] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," *Future Gener. Comput. Syst.*, vol. 82, pp. 12–28, May 2018.

[25] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Veh. Commun.*, vol. 11, pp. 1–11, Jan. 2018.

[26] C. R. Silva, R. O. Moraes, L. H. S. Lelis, and K. Gal, "Strategy generation for multi-unit real-time games via voting," *IEEE Trans. Games*, to be published.

[27] R. Esmaeilyfard, F. Hendessi, M. H. Manshaei, and J. Grossklags, "A game-theoretic model for users' participation in ephemeral social vehicular networks," *Int. J. Commun. Syst.*, vol. 32, no. 12, pp. 1–21, 2019.

[28] F. Hof, W. Kern, S. Kurz, K. Pashkovich, and D. Paulusma, "Simple games versus weighted voting games: Bounding the critical threshold value," *Proc. SSRN*, vol. 3270445, pp. 1–10, Oct. 2018. [Online]. Available: https://www.ssrn.com/index.cfm/en/

[29] A. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust deep reinforcement learning for security and safety in autonomous vehicle systems," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Maui, HI, USA, 2018, pp. 307–312.

[30] A. Behfarnia and A. Eslami, "Risk assessment of autonomous vehicles using Bayesian defense graphs," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, 2018, pp. 1–5.

[31] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, 2013.

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

[33] J. A. Sanguesa, F. Naranjo, V. Torres-Sanz, M. Fogue, P. Garrido, and F. J. Martinez, "On the study of vehicle density in intelligent transportation systems," *Mobile Inf. Syst.*, vol. 2016, pp. 1–13, Jan. 2016, Art. no. 8320756.

ALI BEHFARNIA (S'16) received the B.S. degree in electrical engineering from the University of Tabriz and the M.S. degree in electrical engineering from the Iran University of Science and Technology (IUST). He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science, Wichita State University, KS, USA. He was a recipient of the Bright Future Award from Wichita State Ventures and the Donald D. Sbarra Endowed Fellowship, in 2016. His research interests include resilient cyber-physical systems, error control coding, game theory, applications of machine and deep learning, and communications over wireless networks.

ALI ESLAMI (S'07–M'13) received the Ph.D. degree in electrical and computer engineering from the University of Massachusetts, Amherst, in 2013. From August 2014 to June 2015, he was a Visiting Research Scholar of information initiative at Duke (iiD). He was a Postdoctoral Research Fellow of Texas A&M University, College Station, TX, USA, from March 2013 to April 2015. He is an Assistant Professor of electrical engineering and computer science with Wichita State University, Wichita, KS, USA. His current research interests include nano-communications, applications of coding theory in biology, resilient design of cyber-physical systems, fault-tolerant quantum computing, and big-data storage systems. He is a member of the IEEE Communications and Computer Societies. He was a recipient of the Wichita State's Young Faculty Risk Taker Award, from 2016 to 2017. He has served as the Session Chair for several IEEE conferences and workshops. He has served as a Reviewer for numerous IEEE journals. He has also served on several NSF review panels.