Intrusion Detection for Wireless Sensor Networks: A Multi-Criteria Game Approach

Sanghai Guan*, Jingjing Wang*, Chunxiao Jiang†, Jihong Tong‡, and Yong Ren*
*Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
†Tsinghua Space Center, Tsinghua University, Beijing, 100084, China
‡School of Information Engineering, Eastern Liaoning University, Dandong, Liaoning, 118003, China
Email: gsh17@mails.tsinghua.edu.cn, chinaeephd@gmail.com, jchx@tsinghua.edu.cn,
sam.su@sap.com, reny@tsinghua.edu.cn

***Abstract*—In view of the compelling applications in both military and civilian fields, wireless sensor networks (WSNs) have attracted an unprecedented focus on their easy configuration and low cost. Due to the openness of wireless media and constrained resources of WSNs, it is of paramount importance to timely discern the malicious intrusion and unauthorized manipulation. In this paper, we engage in providing an intrusion detection mechanism relying on a novel multi-criteria game. In our model, the interaction between potential attackers and defenders is formulated as a two-player non-zero-sum multi-criteria game, where multiple objectives, i.e. the information security, reputation and energy consumption, are considered when searching for the Pareto equilibrium. Moreover, a light weighting strategy is proposed in order to construct the payoff vector. Finally, simulation results and theoretical analysis show the effectiveness and feasibility of our proposed mechanism.**

***Index Terms*—Multi-criteria game, Pareto equilibrium, intrusion detection, multi-objective optimization.**

I. Introduction

Recently, wireless sensor networks (WSNs) have constituted a promising subject-area for both military applications and for civilian applications, such as battlefield reconnaissance, health care surveillance, etc. Relying on compactly and unobtrusively distributed autonomous sensors, WSNs are beneficial in terms of constructing a fine-grained monitoring of surrounding physical or environmental conditions. However, exposed to the open and deserted wireless environment, sensor nodes are vulnerable to be manipulated and information may also be eavesdropped by above-mentioned malicious nodes. Hence, a superior intrusion detection system (IDS) [1] and reputation mechanism [2] are conducive to both maintaining the network normal operation and to ensuring information security.

In the literature, game theory [3]–[6] has been widely used in IDSs for safeguarding wireless network security [7]–[12]. Specifically, in [7], Liu *et al.* analyzed the achievable Nash equilibrium in both static and dynamic attacker/defender games. Yu *et al.* presented a joint analysis of cooperation stimulation and security in autonomous mobile ad hoc networks under a game theoretic framework in [8]. Moreover, a Bayesian hybrid detection mechanism was proposed for the defender for monitoring and estimating opponents' actions. Chen *et al.* [9] constructed a game theoretical intrusion detection framework and elaborated the minimum monitor resource requirement as well as the optimal strategy of defenders. Furthermore, in [10], the IDS was formulated as an incomplete information stochastic game and a reinforcement learning based Bayesian Nash-Q learning identification procedure was proposed by He *et al.*

However, the above-mentioned intrusion detection mechanisms focused more on a single objective function (OF), which cannot reflect the contradiction amongst multiple objectives as well as players' trade-off consideration during the decision making process. Multi-objective games achieved significant gains compared with the conventional single-objective game in wireless networks and cyber security. In [13], Duan *et al.* proposed a communication and storage-aware multi-objective algorithm in order to fulfill two constraints, i.e. network bandwidth and storage resources. Stupia *et al.* [14] modeled the power control problem in a Gaussian interference channel as a competitive multi-objective game to make a balance between information rate and energy efficiency. In [15], Eisenstadt *et al.* constituted a multi-objective attack-defence game and its solution for highlighting the applicability and advantage to cyber security.

As for the intrusion detection mechanism in WSNs, on one hand the normal nodes with an IDS concentrate on largely preventing information disclosure in terms of minimum energy consumption. On the other hand, malicious nodes intend to eavesdrop more useful information, yet to maintain a relatively high reputation for avoiding being removed from the network. Hence, information security, nodes' reputation, energy consumption, etc. should be well considered in designing the attack-defense intrusion detection mechanism for WSNs. These challenges give us the motivation to conceive the paper to construct a multi-criteria intrusion detection game for WSNs with the following original contributions.

- Bearing in mind the contradiction among information security, reputation and energy consumption, a two-player multi-criteria game based intrusion detection mechanism is formulated for WSNs, followed by a concrete analysis of its Pareto equilibrium.
- A light weighting strategy is proposed for constructing the payoff vector, which can be a feasible solution for our proposed multi-criteria game.

978-1-5386-1734-2/18/$31.00 ©2018 IEEE

- A toy example is presented. Moreover, the effectiveness of our proposed game is verified by sufficient simulations.

The remainder of this paper is outlined as follows. In Section II, we propose the multi-criteria intrusion detection game model for WSNs. Moreover, we analyze its Pareto equilibrium and a light weighting solution method. Section III presents a toy example of our proposed mechanism and characterizes its performance, followed by our conclusions and future work in Section IV.

II. Multi-Criteria Intrusion Detection Game Model for WSNs

As mentioned above, sensor nodes in WSNs are vulnerable to numerous security threats when exposed in the open wireless environment. In order to detect the attacks from potential malicious nodes, sensor nodes are usually equipped with sorts of IDSs. Moreover, the reputation mechanism is constituted to remove potential malicious nodes and to promote the cooperation in forwarding information. However, sensor nodes are required to be energy efficient in terms of their limited battery power. Hence, in this section, an intrusion detection mechanism for WSNs is elaborated relying on a resilient multi-criteria game model, which takes into account the trade-off between information security, reputation and energy consumption.

A. Game Model

In this subsection, the interaction between a malicious node and a normal node can be modeled as a two-player and non-zero-sum multi-criteria game. Specifically, player 1 and player 2 represent the malicious node and the normal node, respectively. Furthermore, we assume that player 1 has m possible action strategies and an objective payoff of r_1, while player 2 has n possible action strategies with an objective payoff of r_2. Each player will receive a payoff vector when it makes the final decision. Hence, the $m \times n$ payoff matrix of two players, namely $\mathbb{A}$ and $\mathbb{B}$, can be formulated as:

$$\mathbb{A} = \begin{bmatrix} \boldsymbol{a}_{11} & \cdots & \boldsymbol{a}_{1n} \\ \vdots & \ddots & \vdots \\ \boldsymbol{a}_{m1} & \cdots & \boldsymbol{a}_{mn} \end{bmatrix}, \tag{1a}$$

$$\mathbb{B} = \begin{bmatrix} \boldsymbol{b}_{11} & \cdots & \boldsymbol{b}_{1n} \\ \vdots & \ddots & \vdots \\ \boldsymbol{b}_{m1} & \cdots & \boldsymbol{b}_{mn} \end{bmatrix}, \tag{1b}$$

where $\boldsymbol{a}_{ij} = (a_{ij}^1, \ldots, a_{ij}^{r_1})$ and $\boldsymbol{b}_{ij} = (b_{ij}^1, \ldots, b_{ij}^{r_2})$ denote the payoff vectors of player 1 and player 2 in the context of player 1 selecting the pure-strategy $i \in \{1, \ldots, m\}$, while player 2 choosing $j \in \{1, \ldots, n\}$, respectively. The information security, reputation and the energy consumption are considered as the objective variables, i.e. $r_1 = r_2 = 3$. Moreover, the malicious node has $m = 3$ strategies for its action, namely *Attack*, *Idle* and *Cooperate*. As a countermeasure, the normal node with an IDS correspondingly has $n = 3$ strategies for its action, i.e. *Monitor*, *Idle* and *Cooperate*. Hence, the tri-criteria game $(\mathbb{A}, \mathbb{B})$ has been constructed in terms of a pair of payoff matrices represented by $\mathbb{A}_{3\times3}$ and $\mathbb{B}_{3\times3}$, which are detailedly described in Table I and in Table II.

TABLE I
Payoff Matrix of the Tri-Criteria Game

	Monitor	Idle	Cooperate
Attack	$(0, -R_m, -E_a)$, $(0, R_m, -E_m)$	$(S_a, 0, -E_a)$, $(-S_a, 0, 0)$	$(S_a, -R_p, -E_a)$, $(-S_a, 0, -E_c)$
Idle	$(0, 0, 0)$, $(0, 0, -E_m)$	$(0, 0, 0)$, $(0, 0, 0)$	$(0, -R_p, 0)$, $(0, 0, -E_c)$
Cooperate	$(0, 0, -E_c)$, $(0, -R_p, -E_m)$	$(0, 0, -E_c)$, $(0, -R_p, 0)$	$(S_c, R_c, -E_c)$, $(-S_c, R_c, -E_c)$

TABLE II
Parameter Description for the Payoff Matrix

Symbol	Meaning
S_a	Private information eavesdropped under a successful attack
S_c	Private information wiretapped under the bi-cooperation
R_m	Defender's reputation reward when monitoring an attack & Attacker's reputation punishment when its attack monitored
R_p	Reputation punishment of refusing cooperation
R_c	Reputation reward of achieving cooperation
E_a	Attacker's energy consumption during an attack
E_m	Defender's energy consumption during monitoring
E_c	Energy consumption during cooperating

The payoff of the aforementioned two nodes can be determined by their final actions. As shown in Table I, the malicious node (row player) is capable of selecting *Attack* strategy to eavesdrop private information, while the normal node with an IDS (column player) can choose *Monitor* strategy to protect its privacy. Additionally, both nodes may execute *Idle* strategy for reducing energy consumption, or *Cooperate* strategy for restoring their reputation because the node with a flunked reputation will be removed from the network.

Furthermore, under a successful attack, a large amount of private information, which is quantified as S_a, may be eavesdropped by the malicious node. While a small quantity of information of S_c may also be wiretapped under the bi-cooperation scenario because of its forwarding capability. Without loss of generality, we assume that $S_a \gg S_c$.

B. Pareto Equilibrium Analysis

In our multi-criteria game model, the node not only makes a tradeoff between three conflicting objects, but also takes into account the opponent's strategy. In the following, we first define the concept of *Pareto equilibrium* for our proposed multi-criteria game [16].

Definition 1. *The final strategy pair (i^*, j^*) of two players is a pure-strategy Pareto equilibrium, if there is not another pair of strategies that satisfies:*

$$\boldsymbol{a}_{i^*j^*} \preceq \boldsymbol{a}_{ij^*} \quad \textit{and} \quad \boldsymbol{b}_{i^*j^*} \preceq \boldsymbol{b}_{i^*j}, \tag{2}$$

where "$\preceq$" represents "less than or equal to" for every component in a vector as well as "strictly less than" for at least one component in the vector.

As a result, we can obtain the pure-strategy Pareto equilibrium (i^*, j^*) of our game model, where $i, j \in \{1, 2, 3\}$.

The following is the mixed-strategy Pareto equilibrium of our proposed game. According to Eq. (1), we define two submatrices $\boldsymbol{A}_k$ and $\boldsymbol{B}_k$ as:

$$\boldsymbol{A}_k = \begin{bmatrix} a_{11}^k & \cdots & a_{1n}^k \\ \vdots & \ddots & \vdots \\ a_{m1}^k & \cdots & a_{mn}^k \end{bmatrix}, \quad k = 1, \ldots, r_1, \tag{3a}$$

$$\boldsymbol{B}_k = \begin{bmatrix} b_{11}^k & \cdots & b_{1n}^k \\ \vdots & \ddots & \vdots \\ b_{m1}^k & \cdots & b_{mn}^k \end{bmatrix}, \quad k = 1, \ldots, r_2. \tag{3b}$$

Hence, $\mathbb{A}$ and $\mathbb{B}$ of Eq. (1) can be reformulated as $\boldsymbol{A} = (\boldsymbol{A}_1, \ldots, \boldsymbol{A}_{r_1})^T$ and $\boldsymbol{B} = (\boldsymbol{B}_1, \ldots, \boldsymbol{B}_{r_2})^T$. Let $\mathcal{X}$ and $\mathcal{Y}$ denote the strategy space of player 1 and player 2, respectively. Then, we have:

$$\mathcal{X} = \left\{ \boldsymbol{x} = (x_1, \ldots, x_m)^T \middle| \sum_{i=1}^{m} x_i = 1, x_i \geq 0 \, (i = 1, \ldots, m) \right\}, \tag{4a}$$

$$\mathcal{Y} = \left\{ \boldsymbol{y} = (y_1, \ldots, y_n)^T \middle| \sum_{j=1}^{n} y_j = 1, y_j \geq 0 \, (j = 1, \ldots, n) \right\}. \tag{4b}$$

If player 1 selects a mixed-strategy $\boldsymbol{x} \in \mathcal{X}$ and player 2 chooses $\boldsymbol{y} \in \mathcal{Y}$, the expected payoff of both players can be represented as:

$$\boldsymbol{x}^T \boldsymbol{A} \boldsymbol{y} = (\boldsymbol{x}^T \boldsymbol{A}_1 \boldsymbol{y}, \ldots, \boldsymbol{x}^T \boldsymbol{A}_{r_1} \boldsymbol{y}), \tag{5a}$$

$$\boldsymbol{x}^T \boldsymbol{B} \boldsymbol{y} = (\boldsymbol{x}^T \boldsymbol{B}_1 \boldsymbol{y}, \ldots, \boldsymbol{x}^T \boldsymbol{B}_{r_2} \boldsymbol{y}). \tag{5b}$$

Then, according to [17], the mixed-strategy Pareto equilibrium of multi-criteria game $(\boldsymbol{A}, \boldsymbol{B})$ can be defined as follows.

Definition 2. *The strategy pair $(\boldsymbol{x}^*, \boldsymbol{y}^*) \in \mathcal{X} \times \mathcal{Y}$ is a mixed-strategy Pareto equilibrium, if there does not exist another pair of strategies that satisfies:*

$$(\boldsymbol{x}^*)^T \boldsymbol{A} \boldsymbol{y}^* \preceq \boldsymbol{x}^T \boldsymbol{A} \boldsymbol{y}^*, \tag{6a}$$

$$(\boldsymbol{x}^*)^T \boldsymbol{B} \boldsymbol{y}^* \preceq (\boldsymbol{x}^*)^T \boldsymbol{B} \boldsymbol{y}. \tag{6b}$$

Hence, we can achieve the mixed-strategy Pareto equilibrium $\boldsymbol{x}^* = (x_1^*, x_2^*, x_3^*)$ as well as $\boldsymbol{y}^* = (y_1^*, y_2^*, y_3^*)$ of our proposed game.

C. A Light Weighting Solution

At the time of writing, it remains an open challenge to derive the analytical solution space of our proposed multi-criteria game. Additionally, there may exist numerous pure- or mixed-strategy Pareto equilibria, which makes it difficult for the defenders opt for the optimal strategy considering all the possible cases. Therefore, in this subsection we propose a weighting strategy to exploit the reasonable mixed-strategy relying on nodes' prior preference on multiple objectives in order to simplify the calculation.

Based on the linear weighting method, the multi-criteria game $(\boldsymbol{A}, \boldsymbol{B})$ can be degenerated into a single-criteria game, i.e.

$$\boldsymbol{A}(\boldsymbol{w}) = \sum_{k=1}^{r_1} w_k \boldsymbol{A}_k, \quad \text{and} \quad \boldsymbol{B}(\boldsymbol{v}) = \sum_{k=1}^{r_2} v_k \boldsymbol{B}_k, \tag{7}$$

where $\boldsymbol{w} = (w_1, \ldots, w_{r_1}) \in \mathbb{R}_+^{r_1}$, while $\boldsymbol{v} = (v_1, \ldots, v_{r_2}) \in \mathbb{R}_+^{r_2}$. Moreover, $\boldsymbol{w}$ and $\boldsymbol{v}$ can be deemed as the common knowledge of both players. It has been proved that the mixed-strategy Nash equilibrium $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ of the single-criteria game $(\boldsymbol{A}(\boldsymbol{w}), \boldsymbol{B}(\boldsymbol{v}))$ must be a mixed-strategy Pareto equilibrium of the multi-criteria game $(\boldsymbol{A}, \boldsymbol{B})$ [18].

Nevertheless, we still have to determine the exact weight assigned to each objective, which represents its importance to the player. Hence, according to Eq. (7), we define a pair of weighting vectors of $\boldsymbol{w} = (w_1, w_2, w_3)$ and $\boldsymbol{v} = (v_1, v_2, v_3)$, which can be given by:

$$\begin{cases} w_1 = \alpha_1, \\ w_2 = \beta_1 [\Phi_1 - \phi_1]_+, \\ w_3 = \gamma_1 [\Psi_1 - \psi_1]_+, \end{cases} \tag{8}$$

as well as

$$\begin{cases} v_1 = \alpha_2, \\ v_2 = \beta_2 [\Phi_2 - \phi_2]_+, \\ v_3 = \gamma_2 [\Psi_2 - \psi_2]_+, \end{cases} \tag{9}$$

where "$[\cdot]_+$" represents "$\max(\cdot, 0)$", while α_l, β_l and γ_l $(l = 1, 2)$ are the weighting factors of information security, node's reputation and energy consumption, respectively, which are capable of being adjusted by players hinging on their preference. Moreover, ϕ_l denotes player l's current reputation and Φ_l represents its reputation threshold. Furthermore, ψ_l denotes player l's remaining battery power and Ψ_l is its energy threshold. Specifically, the player l will be removed from the network if ϕ_l drops down to zero. Hence, w_2 and v_2 increases with respect to the decrease of ϕ_l, which means that the player t focuses more attention on restoring its reputation when ϕ_l reduces to zero. The same goes for w_3 and v_3 with respect to ψ_l. Therefore, the nodes can adjust their strategies dynamically with the change of status.

D. Repeated Game

In WSNs, it is common that the nodes interact continually, which calls for a repeated game with multiple stages. At the end of each stage, the status of two nodes (i.e., reputation value, residual energy) is changed according to their actions, and the weighting vector $\boldsymbol{w}$ and $\boldsymbol{v}$ will change as well. As a result, we can update the payoff matrices $\boldsymbol{A}(\boldsymbol{w})$ and $\boldsymbol{B}(\boldsymbol{v})$ in the next stage. Therefore, our game model evolves into a stochastic game model in this repeating scenario. Moreover, the payoff matrices of a stage are completely determined by the last stage, which follow the Markovian property. The strategy improvement for a single node can be also regarded as a Markov decision process.

III. Simulation Results

A. A Toy Example

In this section, extensive simulations are conducted in order to evaluate the performance of our proposed game model. Specifically, let $S_a = 25$ kB, $S_c = 2$ kB, $R_m = 15$, $R_p = 2$, $R_c = 5$, $E_a = 5$ mW·h, $E_m = 3$ mW·h and $E_c = 2$ mW·h. Then, the payoff matrix can be rewritten in the form of $(\mathbb{A}, \mathbb{B})$ as shown in Table III.

TABLE III
A Numerical Example

	Monitor	Idle	Cooperate
Attack	$(0, -15, -5)$, $(0, 15, -3)$	$(25, 0, -5)$, $(-25, 0, 0)$	$(25, -2, -5)$, $(-25, 0, -2)$
Idle	$(0, 0, 0)$, $(0, 0, -3)$	$(0, 0, 0)$, $(0, 0, 0)$	$(0, -2, 0)$, $(0, 0, -2)$
Cooperate	$(0, 0, -2)$, $(0, -2, -3)$	$(0, 0, -2)$, $(0, -2, 0)$	$(2, 5, -2)$, $(-2, 5, -2)$

B. Pure-Strategy Pareto Equilibrium

According to Def. 1, there are three pure-strategy Pareto equilibria in this example, i.e., $(\textit{Attack}, \textit{Idle})$, $(\textit{Idle}, \textit{Idle})$ and $(\textit{Cooperate}, \textit{Cooperate})$, where no player can increase all the aspects of payoffs by changing its action unilaterally. However, these equilibria are just "weak" Pareto equilibria, where players can increase part of the aspects of payoffs by changing the action. For example, in equilibrium $(\textit{Attack}, \textit{Idle})$, it is reasonable for the defender to turn to *Monitor* for the security and reputation gain at the expense of energy loss.

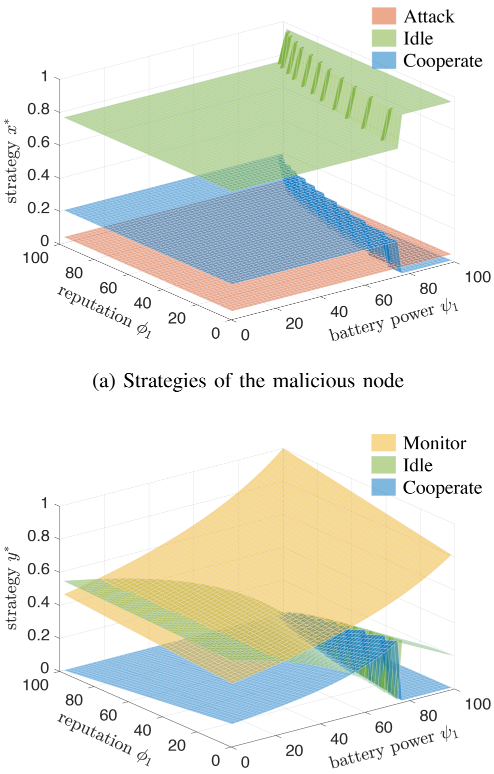
Therefore, the pure-strategy Pareto equilibrium is just non-dominated, and holds weaker stability than that of conventional Nash equilibrium. We can not predict which mentioned-above equilibrium may occur in physical reality, whilst its stability cannot be guaranteed as well. Hence, we will adopt our proposed weighting mechanism to analyze mixed-strategies for a better description of two nodes' tendency of selecting different actions.

C. Mixed-Strategy Pareto Equilibrium

As to the simulation of mixed-strategies, we set the parameters as shown in Table IV.

TABLE IV
Simulation Parameters

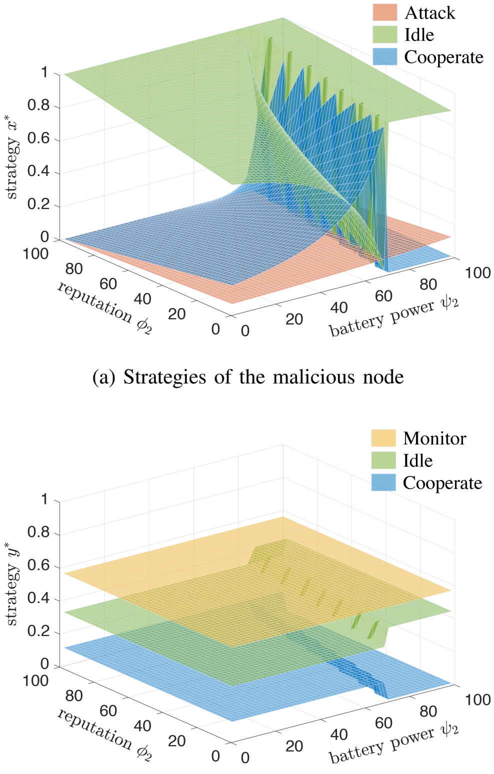
Parameter	Value	Parameter	Value
α_1	1 kB^{-1}	α_2	1 kB^{-1}
β_1	0.02	β_2	0.02
Φ_1	200	Φ_2	200
γ_1	0.01 (mW·h)$^{-1}$	γ_2	0.01 (mW·h)$^{-1}$
Ψ_1	100 mW·h	Ψ_2	100 mW·h



(a) Strategies of the malicious node

(b) Strategies of the normal node

Fig. 1. Mixed-strategy Pareto equilibrium versus different ϕ_1 and ψ_1.



(a) Strategies of the malicious node

(b) Strategies of the normal node

Fig. 2. Mixed-strategy Pareto equilibrium versus different ϕ_2 and ψ_2.

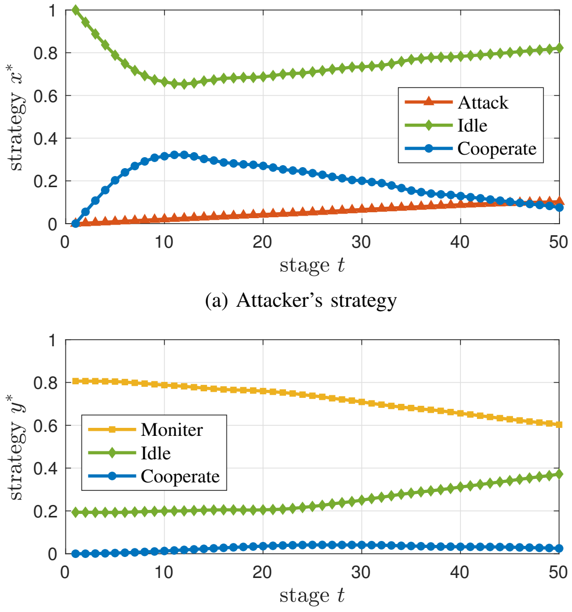
Then, we can get the weighting vectors $\boldsymbol{w}$ and $\boldsymbol{v}$ according to Eq. (8). The mixed-strategy Pareto equilibrium of the malicious node and the normal node is shown in Fig. 1 and Fig. 2, where there may exist multiple mixed-strategy equilibria in some cases. Moreover, the optimum solution is presented in these figures.

Fig. 1a and Fig. 1b illustrate the two nodes' strategies parameterized by different reputation and battery power of the malicious node, i.e. ϕ_1 and ψ_1. Here, we set $\phi_2 = 50$ and $\psi_2 = 50$ mW·h. Firstly, we analyze the probability of selecting different actions for the normal node. The payoff matrix of the malicious node, termed $\boldsymbol{A}(\boldsymbol{w})$, constantly changes. As shown in Fig. 1b, with the increase of ψ_1 and ϕ_1, the normal node increases its probability of monitoring the malicious node to prevent its private information. This is because the malicious node with high battery power and reputation has stronger motivation to choose attack. Moreover, with the increase of ψ_1 and decrease of ϕ_1, the normal node tends to choose cooperation other than staying idle, which promotes the cooperation between nodes and improves the network environment. However, when ϕ_1 increases and ψ_1 is greater than about 80, the original equilibrium no longer exists and the players turn to another equilibrium, where the cooperation probability reduces to zero. In this equilibrium, the malicious node with high battery power and low reputation will be removed from the network. Fig. 1a reveals the equilibrium strategies of the malicious node. It chooses the strategy $(0.04, 0.76, 0.2)$ in most cases, while may turn to the strategy $(0.04, 0.96, 0)$ when ψ_1 is high enough and ϕ_1 is low.

Fig. 2a and Fig. 2b show the two nodes' strategies versus different ϕ_2 and ψ_2. Here we set $\phi_1 = 50$ and $\psi_1 = 50$ mW·h. In this case, the malicious node's payoff $\boldsymbol{B}(\boldsymbol{v})$ does not change and the malicious node's strategies are illustrated in Fig. 2a. With the decrease of normal node's reputation ϕ_2 and the increase of battery power ψ_2, the malicious node tends to choose cooperation and attack, and the probability of staying idle declines rapidly. In this case, the normal node tends to consume energy for cooperation to obtain reputation and the malicious node can take this opportunity to attack or cooperate in order to maximize its payoff. When ψ_1 continues to increase, the original equilibrium does not exist and the two nodes do not choose cooperation any longer, which is similar to Fig. 1b. In addition, as shown in Fig. 2b, the normal node's two equilibrium strategies are $(0.56, 0.33, 0.11)$ and $(0.56, 0.44, 0)$, respectively.

D. Repeated Game Simulation

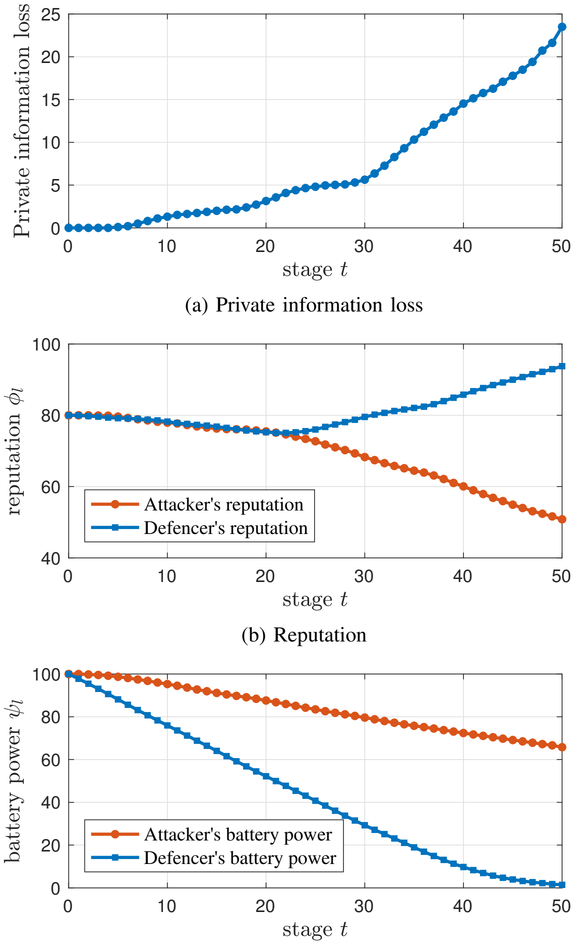
In this subsection, we construct a repeated game with 50 stages for observing the long-term strategies of two nodes. In the simulation, each node selects the action according to the mixed Pareto equilibrium strategy analyzed above. At the beginning of the game, the initial reputation value of nodes is $\phi_1 = \phi_2 = 80$, and their initial battery power $\psi_1 = \psi_2 = 100$mW·h. Other parameters are the same as the previous subsection. Moreover, both kind of nodes only consider the current payoff and select a greedy strategy, i.e.



(a) Attacker's strategy

(b) defender's strategy

Fig. 3. Two nodes' strategies in each stage of the repeated game.



(a) Private information loss

(b) Reputation

(c) Battery power

Fig. 4. Two nodes' status in each stage of the repeated game.

the discount factor equals zero. The simulation is repeated for 50 times to achieve the average results, which are shown in Fig. 3 and Fig. 4.

The status of two nodes at each stage is illustrated in Fig. 4. Firstly, Fig. 4a shows the accumulated private information loss of the regular node, which is also the gain of the malicious node. The average accumulated information loss in 50 stages is 24kB and the miss detection rate is less than 2% according to the simulation parameters, which indicates that the proposed scheme for regular nodes has high security. The information leakage rate is increasing with the decrease of the regular node's battery power and the increase of malicious node's attacking probability. Moreover, the curves in Fig. 4b indicate that malicious node's reputation gradually decreases and the regular of ordinary nodes increases. Therefore, the reputation mechanism is conducive to differentiating the types of the nodes in WSNs, which can protect the regular nodes and remove the malicious nodes from the network. Finally, it is apparent in Fig. 4c that the nodes' battery power decreases as the repeated game goes on. Because the IDS acts frequently under potential attacks, the regular node consumes the power more rapidly than the malicious node and almost depletes its battery power in the last stage. Therefore, in order to enhance the security of WSNs, it is necessary to check and restore the battery power of the nodes.

In addition, Fig. 3a and Fig. 3b show the strategies of malicious nodes and ordinary nodes in different stages of the game. As the game goes on, the probability that the malicious node chooses attack increases gradually. Moreover, the regular node's average detection probability is about 70% and the regular node tends to stay idle rather than to cooperate.

In conclusion, our simulations verify the effectiveness and practicability of our light weighting strategy and simulation results reveal the rationality of both kinds of nodes in this game.

IV. Conclusions and Future Work

In this paper, we proposed a multi-criteria game based intrusion detection model in WSN. We derived and reviewed the pure-strategy Pareto equilibrium of our game model. Moreover, although the analytical solution of our game model remains an open challenge, we deduced the reasonable mixed Pareto equilibrium strategies relying on our preference-based weighting mechanism. In our numerical example, simulation results and corresponding theoretical analysis show the effectiveness and feasibility of our proposed mechanism. In future work, we intend to improve our model to delineate the scenario of dynamic games as well as games with incomplete information in WSNs.

Acknowledgment

This work was supported by the Shenzhen Science and Technology Program (Grant No. JCYJ20150831192224146).

References

[1] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, May. 2014.

[2] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

[3] C. Jiang, Y. Chen, and K. R. Liu, "Multi-channel sensing and access game: Bayesian social learning with negative network externality," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 2176–2188, Apr. 2014.

[4] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, p. 25, Jun. 2013.

[5] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 472–486, Jan. 2013.

[6] C. Jiang, Y. Chen, and K. R. Liu, "Graphical evolutionary game for information diffusion over social networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 4, pp. 524–536, Aug. 2014.

[7] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in *EAI International Conference on Game Theory for Networks*, Pisa, Italy, Oct. 2006, pp. 4–16.

[8] W. Yu and K. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, Mar. 2007.

[9] L. Chen and J. Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 2, pp. 165–178, Jun. 2009.

[10] X. He, H. Dai, P. Ning, and R. Dutta, "Dynamic IDS configuration in the presence of intruder type uncertainty," in *IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, Dec. 2015, pp. 1–6.

[11] J. Wang, C. Jiang, Z. Han, T. Q. Quek, and Y. Ren, "Private information diffusion control in cyber physical systems: A game theory perspective," in *26th IEEE International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, Canada, Jul. 2017, pp. 1–10.

[12] C. Jiang, Y. Chen, Y. Gao, and K. R. Liu, "Joint spectrum sensing and access evolutionary game in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2470–2483, May. 2013.

[13] R. Duan, R. Prodan, and X. Li, "Multi-objective game theoretic scheduling of bag-of-tasks workflows on hybrid clouds," *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, pp. 29–42, Jan. 2014.

[14] I. Stupia and L. Vandendorpe, "Energy efficiency-rate multiobjective game: Tradeoffs, scalarisation techniques and distributed implementation," in *IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, May. 2016, pp. 1–6.

[15] E. Eisenstadt and A. Moshaiov, "Novel solution approach for multi-objective attack-defense cyber games with unknown utilities of the opponent," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 1, pp. 16–26, Feb. 2017.

[16] M. Zeleny, "Games with multiple payoffs," *International Journal of Game Theory*, vol. 4, no. 4, pp. 179–191, Dec. 1975.

[17] I. Nishizaki and T. Notsu, "Nondominated equilibrium solutions of a multiobjective two-person nonzero-sum game and corresponding mathematical programming problem," *Journal of Optimization Theory and Applications*, vol. 135, no. 2, pp. 217–239, Nov. 2007.

[18] L. S. Shapley and F. D. Rigby, "Equilibrium points in games with vector payoffs," *Naval Research Logistics*, vol. 6, no. 1, pp. 57–61, Mar. 1959.