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

Sanghai Guan[1], Jingjing Wang[1], Chunxiao Jiang[2], Jihong Tong[3], and Yong Ren[1]

[1]Department of Electronic Engineering, Tsinghua University, Beijing, China
[2]Tsinghua Space Center, Tsinghua University, Beijing, China
[3]School of Information Engineering, Eastern Liaoning University, Liaoning, China

gsh17@mails.tsinghua.edu.cn, chinaeephd@gmail.com, jchx@tsinghua.edu.cn, sam.su@sap.com, reny@tsinghua.edu.cn

**IEEE WCNC**, April 16, 2018

# Content

# Content

# Introduction

Wireless Sensor Networks (WSNs):

- Fine-grained monitoring.
- Wide application fields.

# Introduction

Wireless Sensor Networks (WSNs):

- Fine-grained monitoring.
- Wide application fields.
- Vulnerable to be manipulated.
- Information may be eavesdropped.

# Introduction

Wireless Sensor Networks (WSNs):

- Fine-grained monitoring.
- Wide application fields.
- Vulnerable to be manipulated.
- Information may be eavesdropped.

In WSNs, **Intrusion detection systems (IDSs)** and **reputation mechanisms** are helpful both to maintain the network normal operation and to ensure **information security**.

# Introduction

- **Game theory** has been widely used in IDSs.
- However, most mechanisms just focused on a **single objective function**.

# Introduction

- **Game theory** has been widely used in IDSs.
- However, most mechanisms just focused on a **single objective function**.
- Challenges:
  - The contradiction among **multiple objectives**.
  - The players' **trade-off** consideration.

## Normal Nodes

- Prevent information disclosure.
- Minimize energy consumption.
- ...

## Malicious Nodes

- Eavesdrop more information.
- Maintain a high reputation.
- ...

# Introduction

Our original contributions:

- In consideration of 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.
- A **toy example** is presented. Moreover, the efficiency of our proposed game is verified by sufficient simulations.

# Content

# Game Model

A two-player and non-zero-sum multi-criteria game:

- Players: malicious node (player 1), normal node (player 2).
- Actions: $m$ actions (player 1), $n$ actions (player 2).
- Payoffs: $r_1$ objectives (player 1), $r_2$ objectives (player 2).

# Game Model

A two-player and non-zero-sum multi-criteria game:

- Players: malicious node (player 1), normal node (player 2).
- Actions: $m$ actions (player 1), $n$ actions (player 2).
- Payoffs: $r_1$ objectives (player 1), $r_2$ objectives (player 2).

Hence, the $m \times n$ payoff matrix of two players, namely $\mathbb{A}$ and $\mathbb{B}$, can be formulated as:

$$\mathbb{A} = \begin{bmatrix} \boldsymbol{a}_{11} & \cdots & \boldsymbol{a}_{1n} \\ \vdots & \ddots & \vdots \\ \boldsymbol{a}_{m1} & \cdots & \boldsymbol{a}_{mn} \end{bmatrix} \quad \text{and} \quad \mathbb{B} = \begin{bmatrix} \boldsymbol{b}_{11} & \cdots & \boldsymbol{b}_{1n} \\ \vdots & \ddots & \vdots \\ \boldsymbol{b}_{m1} & \cdots & \boldsymbol{b}_{mn} \end{bmatrix},$$

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.

# Game Model

Table: Payoff Matrix of the Tri-Criteria Game $(\mathbb{A}, \mathbb{B})$

| | 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 | $(0, 0, -E_c)$, $(0, -R_p, -E_m)$ | $(0, 0, -E_c)$, $(0, -R_p, 0)$ | $(S_c, R_c, -E_c)$, $(-S_c, R_c, -E_c)$ |

The malicious node has $m = 3$ strategies: **Attack**, **Idle** and **Cooperate**. The normal node has $n = 3$ strategies: **Monitor**, **Idle** and **Cooperate**.

# Game Model

Table: 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 information security, reputation and the energy consumption are considered as the objective variables, i.e. $r_1 = r_2 = 3$.

# Game Model

Table: Payoff Matrix of the Tri-Criteria Game $(\mathbb{A}, \mathbb{B})$

| | 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 | $(0, 0, -E_c)$, $(0, -R_p, -E_m)$ | $(0, 0, -E_c)$, $(0, -R_p, 0)$ | $(S_c, R_c, -E_c)$, $(-S_c, R_c, -E_c)$ |

The malicious node has $m = 3$ strategies: **Attack**, **Idle** and **Cooperate**. The normal node has $n = 3$ strategies: **Monitor**, **Idle** and **Cooperate**.

# Pareto Equilibrium Analysis

- In the multi-criteria game model, the node has to not only make a tradeoff between three conflicting objects, but also take the opponent's strategy into consideration.
- Firstly, we will give the concept of **Pareto equilibrium** for our proposed multi-criteria game.

## Definition (Pure-Strategy Pareto Equilibrium)

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

$$\boldsymbol{a}_{i^*j^*} \preceq \boldsymbol{a}_{ij^*} \quad \text{and} \quad \boldsymbol{b}_{i^*j^*} \preceq \boldsymbol{b}_{i^*j}.$$

# Pareto Equilibrium Analysis

The following is the mixed-strategy Pareto equilibrium of our proposed game. Here we define two **sub-matrices** $\boldsymbol{A}_k$ and $\boldsymbol{B}_k$ as:

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

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

Hence, $\mathbb{A}$ and $\mathbb{B}$ can be reformulated as $\boldsymbol{A} = (\boldsymbol{A}_1, \ldots, \boldsymbol{A}_{r_1})^T$ and $\boldsymbol{B} = (\boldsymbol{B}_1, \ldots, \boldsymbol{B}_{r_2})^T$.

# Pareto Equilibrium Analysis

Let $\mathcal{X}$ and $\mathcal{Y}$ denote the **strategy space** of two players, i.e.,

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

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

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

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

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

# Pareto Equilibrium Analysis

Then, the **mixed-strategy Pareto equilibrium** of multi-criteria game $(\boldsymbol{A}, \boldsymbol{B})$ can be defined as:

## Definition (Mixed-Strategy Pareto Equilibrium)

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:

$$(\boldsymbol{x}^*)^T \boldsymbol{A}\boldsymbol{y}^* \preceq \boldsymbol{x}^T \boldsymbol{A}\boldsymbol{y}^* \quad \text{and} \quad (\boldsymbol{x}^*)^T \boldsymbol{B}\boldsymbol{y}^* \preceq (\boldsymbol{x}^*)^T \boldsymbol{B}\boldsymbol{y}.$$

# A Light Weighting Solution

- It remains an **open challenge** to derive the analytical solution space of multi-criteria games.
- There may exist **numerous pure- or mixed-strategy Pareto equilibria**, which makes it difficult for the defenders choose the optimal strategy considering all the possible cases.
- Therefore, a **weighting strategy** is proposed to find the reasonable mixed-strategy relying on nodes' prior preference on multiple objectives in order to simplify the calculation.

# A Light Weighting Solution

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

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

where $\boldsymbol{w} = (w_1, \ldots, w_{r_1}) \in \mathbb{R}_+^{r_1}$, while $\boldsymbol{v} = (v_1, \ldots, v_{r_2}) \in \mathbb{R}_+^{r_2}$.

- Weighting vectors $\boldsymbol{w}$ and $\boldsymbol{v}$ can be deemed as the **common knowledge** of both players.
- 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 $(\boldsymbol{A}, \boldsymbol{B})$.

# A Light Weighting Solution

In our weighting mechanism, weighting vectors $\boldsymbol{w} = (w_1, w_2, w_3)$ and $\boldsymbol{v} = (v_1, v_2, v_3)$ are defined as:

$$\begin{cases} w_1 = \alpha_1, \\ w_2 = \beta_1[\Phi_1 - \phi_1]_+, \\ w_3 = \gamma_1[\Psi_1 - \psi_1]_+, \end{cases} \quad \text{and} \quad \begin{cases} v_1 = \alpha_2, \\ v_2 = \beta_2[\Phi_2 - \phi_2]_+, \\ v_3 = \gamma_2[\Psi_2 - \psi_2]_+, \end{cases}$$

- $[\cdot]_+$ $\max(\cdot, 0)$.
- $\alpha_l$, $\beta_l$, $\gamma_l$ The **weighting factors** of information security, node's reputation and energy consumption for player $l$.
- $\phi_l$, $\psi_l$ Player $l$'s **current** reputation and battery power.
- $\Phi_l$, $\Psi_l$ The **threshold** of reputation and energy for player $l$.

# Repeated Game

In WSNs, it is common that the nodes interact continually, which leads to a **repeated game** with multiple stages:

- At the end of a stage, the status of two nodes is changed according to their actions, and the weighting vectors $\boldsymbol{w}$ and $\boldsymbol{v}$ will change as well.
- As a result, we can get new payoff matrices $\boldsymbol{A}(\boldsymbol{w})$ and $\boldsymbol{B}(\boldsymbol{v})$ in the next stage.
- The game model evolves into a **stochastic game** model in this repeating scenario, which possess the Markovian property.

# Content

# A Toy Example

- In the toy example, we take $S_a = 25$ 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 $(\mathbb{A}, \mathbb{B})$ can be rewritten as:

Table: 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 | $(0, 0, -2)$, $(0, -2, -3)$ | $(0, 0, -2)$, $(0, -2, 0)$ | $(2, 5, -2)$, $(-2, 5, -2)$ |

# Pure-Strategy Pareto Equilibrium

There are three **pure-strategy Pareto equilibria** in this example, i.e., $(Attack, Idle)$, $(Idle, Idle)$ and $(Cooperate, Cooperate)$, where no player can increase all objects' payoffs by changing its action unilaterally.

- These equilibria are just "weak" Pareto equilibria, where players can increase partial payoffs.
- Therefore, the pure-strategy Pareto equilibrium is just non-dominated, and holds weak stability.

# Mixed-Strategy Pareto Equilibrium

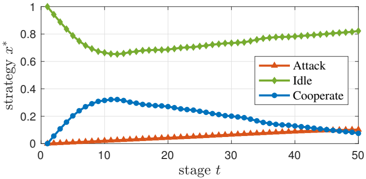
- As a result, we will adopt our proposed weighting mechanism to analyze mixed-strategies for a better description of two nodes' tendency of selecting different actions.
- In the simulation of mixed-strategies, we assume that $\alpha_1 = \alpha_2 = 1\ \mathsf{kB}^{-1}$, $\beta_1 = \beta_2 = 0.02$, $\Phi_1 = \Phi_2 = 200$, $\gamma_1 = \gamma_2 = 0.01\ (\mathsf{mW{\cdot}h})^{-1}$ and $\Psi_1 = \Psi_2 = 100\ \mathsf{mW{\cdot}h}$.
- The most reasonable solution is shown in the figures when there exists multiple mixed-strategy equilibria.

# Repeated Game Simulation

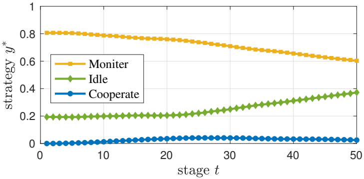
In repeated game simulation, we construct a repeated game with $50$ stages to observe the long-term strategies of two nodes.

- Each node selects the action according to the mixed Pareto equilibrium strategy analyzed above.
- The nodes are with the initial reputation value $\phi_1 = \phi_2 = 80$, and the initial battery power $\psi_1 = \psi_2 = 100\text{mW}\cdot\text{h}$. The other parameters are same as previous.
- Both nodes only consider the current payoff and act a greedy strategy, i.e., the discount factor equals zero.

# Repeated Game Simulation



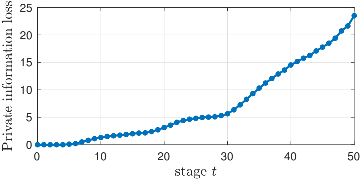

(a) Attacker's strategy



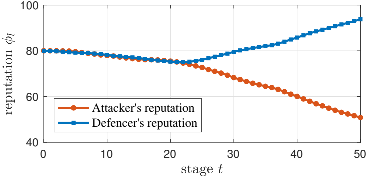

(b) Defender's strategy

Figure: Two nodes' strategies in each stage of the repeated game.

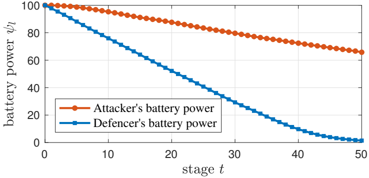
# Repeated Game Simulation




(a) Private information loss




(b) Reputation




(c) Battery power

Figure: Two nodes' status in each stage of the repeated game.

# Repeated Game Simulation

- The proposed scheme for regular nodes has high security.
- The reputation mechanism contributes to differentiate the types of the nodes in WSNs, which can protect the regular nodes and remove the malicious nodes from the network.
- In order to enhance the security of WSNs, it is necessary to check and restore the battery power of the nodes.

# Repeated Game Simulation

- The proposed scheme for regular nodes has high security.
- The reputation mechanism contributes to differentiate the types of the nodes in WSNs, which can protect the regular nodes and remove the malicious nodes from the network.
- In order to enhance the security of WSNs, it is necessary to check and restore the battery power of the nodes.

In conclusion, the simulation above verifies the **effectiveness and practicability** of our weighting strategy, and the results reveal the **rationality** of both nodes in this game.

# Content

# Conclusions and Future Work

**Conclusions**:

- Proposed a multi-criteria game based intrusion detection model in WSN.
- Deduced the pure-strategy and mixed strategy Pareto equilibriums of our model.
- Simulation results and corresponding theoretical analysis showed the efficiency and feasibility of our preference-based weighting mechanism.

# Conclusions and Future Work

Conclusions:

- Proposed a multi-criteria game based intrusion detection model in WSN.
- Deduced the pure-strategy and mixed strategy Pareto equilibriums of our model.
- Simulation results and corresponding theoretical analysis showed the efficiency and feasibility of our preference-based weighting mechanism.

**Our future work:**

- Improve our multi-criteria model to reveal the scenario of dynamic games.
- Discuss intrusion detection games with incomplete information in WSNs.

# Thank You