Article

Tactile Routing for Location Privacy Preservation in Wireless Sensor Networks: A Game Theoretic Approach

Mujahid N. Syed 1,* and Uthman Baroudi 2

1 Interdisciplinary Research Center for Intelligent and Secure Systems, Department of Industrial Systems Engineering, King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia
2 Interdisciplinary Research Center for Smart Cities and Logistic, Department of Computer Engineering, King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia; ubaroudi@kfupm.edu.sa
* Correspondence: smujahid@kfupm.edu.sa or snnumujahid@gmail.com

Abstract: Location Privacy Preservation (LPP) in Wireless Sensor Networks (WSNs) during the era of the Internet of things and smart systems is a critical element in the success of WSNs. LPP in WSN can be stated as: given a WSN with an adversary aiming to unravel the location of critical nodes of a WSN, the goal of the WSN manager is to enshroud the location of the critical nodes via routing and/or encryption mechanisms. Typical research in the LPP of WSN routing involves developing and/or estimating the performance of a fixed routing protocol under a given attack mechanism. Motivated by advancements in network softwarization, in this work, we propose an approach where the WSN manager as well as the WSN adversary can deploy multiple routing and attack mechanisms, respectively. Initially, the proposed approach is formulated as a repeated two-player zero-sum game. The formulation is further extended to handle multiple objectives and incomplete information in the game matrix. In this work, the multiple objectives are handled via the epsilon constraint method. The presence of incomplete information in the formulation is modeled as interval based uncertainty. To sum, the proposed formulation ultimately boils down to linear programming problems, which can be efficiently solved. Numerical case studies to showcase the applicability of the proposed approach are illustrated in this work. Finally, discussion on obtaining the required data from any given WSN, discussion and interpretation of the formulation’s results, and future research direction of the current work is presented.

Keywords: wireless sensor networks; location privacy preservation; game theory; incomplete information in payoffs

1. Introduction

The Internet of things (IoT) is the heart of Industry 4.0, where a number of smart devices are deployed on a communication network. The devices process the incoming and outgoing data ubiquitously, and they communicate among themselves autonomously. Thus, IoT is the crux in developing new applications and experiences including smart factories, smart agriculture, smart homes, etc. The smart devices of IoT play key roles in collecting, processing, and forwarding data from sources nodes to the sink node(s) via multiple hop network communication. This ubiquitous and autonomous communication results in Wireless Sensor Networks (WSNs) with new challenges that are related to their sustainability. On one hand, since these devices are of constrained capabilities such as energy supply, transmission, range, computing power, etc., lots of research works focus on developing routing methods that cope with these devices. On the other hand, these networks are typically deployed and operated in unattended environments. Therefore, these networks might be vulnerable to various type of attacks that may impact the operation of the network partially or completely, such as identifying the location of critical network nodes (such as source(s) and sink(s) nodes). Securing the location of critical nodes in WSNs is a complicated, pressing challenge that needs to be tackled on different fronts.
The seminal work presented in [1] highlights the importance of the Location Privacy Preservation (LPP) of critical nodes in a WSN. Specifically, the authors depicted, via an example of Panda–Hunter Game, the importance of LPP. For example, a habitat containing pandas is monitored via many wireless sensor nodes that are randomly distributed across the habitat. The sensor (source) nodes monitor and send information about pandas to a base (sink) node. The information received at the base station can be used for the well-being of pandas, which can be indirectly achieved by identifying the location of the source nodes. Thus, the hunter moves into the habitat and monitors the network traffic. Tracing the network communication packets (even without actually looking inside the packet) can reveal the location of the source nodes, thereby compromising the location of pandas. Thus, LPP routing methods are critical along with the packet encryption methods.

In this work, we focus on improving routing methods under the assumption that the adversary (generalized term for the hunter in the above example) lacks the ability to decipher the encrypted packets. The conventional research on LPP in WSNs typically assumes a specific intrusion model, and the primary goal is to develop a corresponding routing method that is better in terms of location privacy. In addition to that, the secondary goals may include: reduced age of information and energy consumption. One of the naive assumptions in the conventional approaches is the prepossession of a specific intrusion model. Since the intrusion can be executed by one or more adversaries, surviving one or more intrusion techniques with one specific routing method may not be fruitful in preserving the location of the critical nodes over the network’s time horizon.

Motivated by the advent of network softwarization and advancements in the Soft Defined Network (SDN) and Network Functions Virtualization (NFV) [2,3], our goal is to propose and develop a hybrid routing model where the network communications are carried out via multiple routing mechanisms. Such a tactile routing model provides the means to handle multiple intrusions via multiple techniques. Later, we discuss the applicability of this approach in real networks.

The rest of the paper is organized as follows. Section 2 presents the relevant literature on WSN routing and attack mechanisms. The problem statement is established in Section 3. A connection between the proposed LPP problem and game theory is highlighted in Section 4. Section 5 illustrates relevant experiments, and provides discussion on the experiment data and results. Section 6 concludes the paper.

2. WSN Routing and Attack Mechanism

The LPP for WSNs first appeared in [1]. With the development of IIoTs and extensive applicability of WSNs, the topic of LPP has received widespread attention in the recent decade. Well-known routing ideas available in the LPP literature are categorized as:

**Random Walk Routing:** In this routing, packets are sent from source node to sink node over random walks or paths [4,5]. This is one of the simplest forms of routing, where the sensor nodes do not calculate or store much information. However, this routing often leads to high overall energy consumption due to longer source-to-sink path length [6]. Typically, random walk routing is deployed with additional protocols. For example, see [7–9], which involves random walk routing with other routing methods.

**Phantom Routing:** In this routing, packets are sent from source node to sink node in two phases [1,10]. In the first phase, the packets are sent from source node to phantom node (a node in the network that is typically neither a source nor a sink). In the second phase, the packets are sent from the phantom node to sink node. Typically, in the first phase, random walk routing is used, and in the second phase, shortest path routing is used. The usage of multiple phantom nodes is proposed in [11]. The key difficulty of phantom routing is the selection of phantom nodes. A technique based on sector domain to increase positional diversity of phantom nodes is proposed in [12].

**Fake Packets Routing:** In this routing, along with the real packets, the network is induced with fake packets. The idea is to camouflage real packets among the fake packets. The key
difficulty in this routing is the right number of fake packets to be induced into the network. Furthermore, fake packets consume network resources, including energy and time. Applications of fake packets can be seen in [13,14].

**Ring Routing:** The idea in this routing (see [15]) is to induce disjoint rings (cycles) while transmitting the packets from source nodes to sink node(s). Every disjoint ring contains a master node (bus node) that is responsible for forwarding the packets from source node to sink node (actual route). Simultaneously, the bus nodes on the actual route send additional packets to a ring of nodes. This additional set of packets sent on the disjoint rings confuses the adversaries. The further applications of ring routing can be seen in [16], and energy efficient ring routing can be seen in [17].

**Multi-Path Routing:** In multi-path routing, data between source and sink nodes are sent via multiple disjoint paths. In order to avoid tracing back of the paths by the adversary, some deviation mechanisms are proposed. For example, a random stride routing is proposed in [18], and a constrained random routing is proposed in [19]. The constrained routing limits the energy usage in the network. Typically, multi-path routing without careful deployment suffers from high energy consumption during the transmission. Thus, several flavors of this category focusing on reduced energy consumption in multi-path routing are proposed in [20–22].

**Network Encoded Routing:** In this routing, packets are re-encoded, split into multiple small packets, or integrated into one big packet during the transmission.

**Directional Routing:** Directional routing consists of directional antennas and/or transceivers. The underlying assumption is that the directional routing makes eavesdropping expensive. In [23], the usage of directional antennas along with transmitting power control and information compression is depicted. More usage of directional transceivers is presented in [24].

**Data Mule Routing:** Data mules are nothing but mobile agents. The routing mechanism is as follows: a source node sends packet to a randomly selected intermediate node. The intermediate node forwards the packet to a data mule. The data mule randomly moves around the network and forwards the packet to another intermediate node. Finally, the intermediate node forwards the packet to the sink node. The data mule makes it difficult for adversaries to locate the critical nodes, but it increases the transmission time.

**Context-Aware Routing:** The idea here is to use sensor nodes that can detect and localize the adversary. Such a mechanism can then be used for local temporary shutdown (stop working for a while) of nodes around the adversary [25,26]. This shutdown acts as an entrapment of the adversary. Moreover, based on the distance of adversary from the source or sink nodes, alternate routes avoiding the adversary’s coverage area can be used.

### 3. Problem Statement

Consider a Wireless Sensor Network (WSN) where an adversary makes passive attacks to identify (or locate) the critical nodes. The adversary is free to choose any attack mechanisms, including, for example:

- Eavesdropping.
- Tracing Back.
- Traffic Analysis.
- Node Compromised.
- ID Analysis.
- Collusion Stacks.

Let $A$ be the set of attacking mechanisms available with the adversary and $a \in A$ be an attack mechanism. It is assumed that the adversary is capable of launching local or hotspot-level attacks on the WSN. The goal of the WSN manager is to maximize the safety period, while ensuring the Quality of Service (QoS) with reasonable energy consumption. In this work, we assume that the WSN is designed such that multiple routing mechanisms can adaptively be employed, so the WSN manager (defender) could command the nodes in a WSN to choose among these different routing mechanisms. For example, the WSN
manager (defender) could choose any of the following routing mechanisms for a certain period, and then choose another one for the next period, and so on according to a specific defense strategy:

- Random Walk.
- Ring Routing.
- Phantom Base Station.
- Fake Packet Injection.
- Multi-path Routing.
- Data Mule.
- Hiding Mechanism.
- Directional Communication.
- Isolation Mechanism.

Let $D$ be the set of options available with the defender and $d \in D$ be a defense mechanism. Let $h_{d,a}$ be the total survival time (the time from the start of attacks to the detection of critical station(s)) when the adversary picks an attack mechanism $a$ and the defender picks a defense mechanism $d$. The primary goal of the defender is to have high survival time, which is contrary to the goal of the adversary. Therefore, the payoff for the adversary conflicts with the defender and can be taken as $-h_{d,a}$. Thus, the conflict between adversary and defender can be modeled as a two-player zero sum-game. However, unlike the conventional game theory models, the manager has to satisfy the QoS and energy requirements. In addition to that, the data of survival time may contain uncertainty. All the notations that are used in this paper are defined in Abbreviations. In the following section, a game-theory-based approach to LPP is proposed.

4. Modeling WSN LPP as a Matrix Game

The relation between network designers/administrators and intruders/attackers can be modeled as a non-cooperative game. Hence, security- and privacy-based protocols in computer networks can be designed using game theory. Game-theory-based approaches related to privacy in Internet-based communications can be seen in works [27–32]. In this work, a strategic game between the WSN manager (as the defender) and the WSN attacker (as the adversary) is proposed. The roles of the defender and the adversary, under mild assumptions, can be cast as a two-player zero-sum game. The following are the key assumptions and characteristics of the proposed game:

- Rational players: Both players have well-defined individual goals, and they strive to reach their goals.
- Non-cooperative players: Both players are competitive, and their individual goals are diametrically opposed.
- Finite moves: Both players have a finite set of moves to play. A move for the defender (adversary) can be defined as a selection of a routing (counterattack) mechanism.
- Independent moves: Unlike typical two-player games, in this game, there are no fixed time points where the players play their moves. Practically, the players can play the moves asynchronously and at different frequencies. However, the moves are taken independently, i.e., no player knows the choice of the other player a priori.
- Memory-less repeated moves: The game is a multiple-shot game, where the moves of the defender are not at all visible to the adversary (and vice versa), even after the end of the game. Thus, it exhibits memory-less nature, where none of the players learn from the other based on the past shots or moves.
- Expected preference: For every combination of defender move and attacker move, a payoff is known or can be estimated. This payoff captures the preference relation for each player. Both players prefer to obtain the best of the expected payoff value.

Thus, due to the above nature of the game, it can be approximated as a steady-state, two-player zero-sum game [33]. Since the moves are taken by the players over and over again during the network’s operation, it is advisable for the defender to use different pure
strategies on each move. Therefore, the optimal mixed strategy obtained from the two-player zero-sum game can be utilized as tactical operational probabilities for the defender.

4.1. Deterministic Survival Times

Let $H \in \mathbb{R}^{D \times A}$ be a matrix, where the $d$th row and $a$th column element $h_{d,a}$ represents the survival time when an adversary picks an attack mechanism $a \in A$ and a defender picks a defense mechanism $d \in D$. Let us assume that $h_{d,a}$ is crisp and deterministic. The expected payoff $E$ of the game, gain for the defender (loss for the adversary), is given as follows:

$$E = x^T H y$$

where $x = [x_1, \ldots, x_{|D|}]^T$, $x_d$ is the probability of using the strategy $d$ by the defender, $y = [y_1, \ldots, y_{|A|}]^T$, and $y_a$ is the probability of using the strategy $a$ by the adversary. In the case of mixed strategies, the objective of the defender is to maximize the minimum expected payoff, whereas the objective of the adversary is to minimize the maximum expected payoff.

**Lemma 1.** The Operations Research (OR) model to identify the best mixed strategy for the defender (also known as max-minimizer) can be written as:

$$\max : \min_{x \geq 0} \left\{ x^T H y \right\}$$

where $h_a$ is the ath column of matrix $H$, $e$ represents a vector containing all ones, and its size can be identified from the context.

**Proof 1.** Let $E_d(x)$ be the worst expected payoff value of the defender for any arbitrary choice of $x$, defined as:

$$E_d(x) = \min_{y \geq 0} \{ x^T H y \}$$

The worse expected value can be re-written as:

$$E_d(x) = \min_{y \geq 0} \{ x^T H y \}$$

$$= \min_{y \geq 0} \{ \sum_{a \in A} (H^T x)_a y_a \}$$

$$= \min_{a \in A} \{ (H^T x)_a \}$$

$$= \min_{a \in A} \{ h_a^T x \}$$

where $(H^T x)_a$ is the ath element of vector $H^T x$. Equation (4c) follows from the theory of linear programming, which states that the optimal solution of a linear function $\sum_{a \in A} (H^T x)_a y_a$ on a non-empty simplex $\{ e^T y = 1, y \geq 0 \}$ lies at one of the $|A|$ extreme points. Thus, the OR model that provides the best mixed strategy for the defender (also known as max-minimizer) can be written as:

$$\max : \min_{e^T x = 1, x \geq 0} \left\{ h_a^T x \right\}$$

The above formulation is the same as Formulation (2). \(\Box\)

**Corollary 1.** The OR model to identify the best mixed strategy for the attacker can be written as:

$$\min \left\{ \max_{y \geq 0} \{ h_a^T y \} \right\}$$
where $h_d$ is the $d$th row of matrix $H$.

Lemma 2. The proposed game has a mixed strategy Nash equilibrium.

Proof 2. Based on the linear programming’s weak duality theory [34], the following holds:

$$
\min_{a \in A} \{ h_d^T x | e^T x = 1, x \geq 0 \} \leq \max_{d \in D} \{ h_d^T y | e^T y = 1, y \geq 0 \}
$$

(7)

Notice that both Formulations (2) and (6) are feasible. From the linear programming’s strong duality theory, it can be concluded that the optimal objective values for both formulations are equal and finite, say $v$. That is, the following holds:

$$
\max : \begin{array}{c}
\sum_{d \in D} \{ h_d^T y | e^T y = 1, y \geq 0 \} = v
\end{array}
$$

(8)

Let $x^*$ and $y^*$ be defined as follows:

$$
x^* = \arg\max_{x \geq 0} \left\{ \min_{a \in A} \{ h_d^T x | e^T x = 1 \} \right\}
$$

(9)

$$
y^* = \arg\min_{y \geq 0} \left\{ \max_{d \in D} \{ h_d^T y | e^T y = 1 \} \right\}
$$

(10)

Equation (8) indicates that, no matter what the adversary (defender) chooses to play, the defender (adversary) has no rational to change from $x^*$ ($y^*$). That is, neither can hope to improve the expected payoff value of $x^T H y^*$. Thus, $(x^*, y^*)$ represents the mixed strategy Nash equilibrium of the proposed game. \qed

In practical scenarios, the defender (adversary) may have additional objectives that are unrelated to the adversary (defender). For example, the defender might be inclined to deviate from the optimal mixed strategy in order to reduce energy consumption and/or improve QoS in communication. Formulation (2) can be extrapolated to include the QoS and energy objectives. Incorporation of the additional objectives for the defender’s model may invalidate the above minimax equality. However, the resulting strategy will ensure that QoS and energy consumption in the communication network are at the preferred level. A Multi-Objective Linear Programming (MOLP) model that captures optimal mixed strategy for the defender can be written as:

$$
\max.:
\begin{cases}
\lambda, -q^T x, -p^T x
\end{cases}
$$

(11a)

s.t.:

$$
\begin{align*}
\lambda & \leq h_a^T x & a \in A \\ e^T x & = 1 \\ x & \geq 0
\end{align*}
$$

(11b)(11c)(11d)

where the QoS level expressed in terms of the transmission latency, obtained by strategy $d$, is represented by $q_d$ for all $d \in D$, and $q = [q_1, \ldots, q_D]^T$. Similarly, the energy consumption for strategy $d$ is represented by $p_d$ for all $d \in D$, and $p = [p_1, \ldots, p_D]^T$. Constraints (11c) and (11d) ensure that $x$ results in the probability of selecting the defense strategy. Constraint (11b) along with the first objective in Function (11a) maximizes the worst case survival time. The other two objective functions correspond to transmission latency and energy minimization.

Let $p_{max} = p^T x^*$ and $q_{max} = q^T x^*$. Formulation (11a–d) can be equivalently solved as a series of the following OR models, where $\epsilon_1$ and $\epsilon_2$ are parameters that are selected a priori:
max.:  
\[ \lambda \]  
s.t.:  
\[ \lambda \leq h_{a}^{T}x \quad a \in A \]  
\[ e^{T}x = 1 \]  
\[ q^{T}x \leq q_{\text{max}} - \varepsilon_{1} \]  
\[ p^{T}x \leq p_{\text{max}} - \varepsilon_{2} \]  
\[ x \geq 0 \]  

When \( \varepsilon_{1} = \varepsilon_{2} = 0 \), the solution of Formulation (12a–f) results in minimax game value. However, when \( \varepsilon_{1} \neq 0 \) or \( \varepsilon_{2} \neq 0 \), then the solution deviates from the minimax game value. Obtaining the solution for various values of \( \varepsilon_{1} \) and \( \varepsilon_{2} \) results in a Pareto surface, which can be presented to the WSN manager. The network manager and decision makers can then select the operational point from the Pareto. In the following subsection, we extend the proposed model to handle uncertainty in the \( H \) matrix.

### 4.2. Incomplete Information of Survival Times

Uncertainty in \( H \) matrix is typically referred as incomplete information in payoffs. Both probabilistic and non-probabilistic methods that handle uncertainty in payoffs are available in the literature [35–39]. Uncertain payoffs in the form of interval-valued payoffs [40–43] are related to the proposed WSN game.

In this work, we assume that the uncertainty in estimating parameter \( H \) exists. Furthermore, we assume that the uncertainty can be represented by a bounded interval. Without loss of generality, let the interval based payoff matrix of defender be expressed as \( \Omega = (\omega)_{d,a} = ([h_{d,a}, \bar{h}_{d,a}]) \), where \( (\omega)_{d,a} \) is a closed interval, \( h_{d,a} \) is the lower bound on the closed interval, and \( \bar{h}_{d,a} \) is the upper bound of the closed interval.

Note that the above uncertainty keeps the zero-sum nature of the game intact, since the payoff matrix of the attacker will be nothing but \(-\Omega = (-\omega)_{d,a} = ([\bar{h}_{d,a}, h_{d,a}])\). Similar to the methodology presented in [41] for handling interval-based uncertainty, we transform Formulation (12a–f) into two formulations: one for obtaining lower bound (pessimistic game) and another for obtaining upper bound (optimistic game). The formulations are as follows:

max.:  
\[ \bar{\lambda} \]  
s.t.:  
\[ \bar{\lambda} \leq \bar{h}_{a}^{T}x \quad a = 1, \ldots, A \]  
\[ e^{T}x = 1 \]  
\[ q^{T}x \leq \bar{q}_{\text{max}} - \varepsilon_{1} \]  
\[ p^{T}x \leq \bar{p}_{\text{max}} - \varepsilon_{2} \]  
\[ x \geq 0 \]
max: 
\[ \lambda \]

s.t.: 
\[ \lambda \leq h_a^T x \quad a = 1, \ldots, A \]  
\[ e^T x = 1 \]  
\[ q^T x \leq q_{\text{max}} - \varepsilon_1 \]  
\[ p^T x \leq p_{\text{max}} - \varepsilon_2 \]  
\[ x \geq 0 \]

where the values of \( q_{\text{max}}, p_{\text{max}} \) and \( q_{\text{max}}, p_{\text{max}} \) are obtained using (9) by replacing \( h_a^T \) with \( h_a \) and \( h_a \), respectively. Upon solving Formulations (13a–f) and (14a–f), we obtain the upper bound \( \lambda \) and the lower bound \( \lambda \), respectively, for a given value of \( \varepsilon_1 \) and \( \varepsilon_2 \). To obtain the Pareto surfaces, a grid search on different values of \( \varepsilon_1 \) and \( \varepsilon_2 \) is conducted. The solution of the above two models results in two Pareto surfaces. The network manager and/or the decision maker can pick a desired operational point from the Pareto surfaces.

5. Numerical Experiments and Discussion

In this section, three case studies are presented to illustrate the usage of the proposed approach. Case Study-1 is a toy example that highlights the notion of mixed strategy, steady state analysis, and data estimation. In Case Study-2, synthetic data on an arbitrary 6 × 6 game are utilized to depict the applicability of the proposed game. In Case Study-3, a non-square game with overlapping intervals, which is most likely related to the real-world scenarios, is presented.

5.1. Case Study-1

As a toy example, let us consider the case where a defender can pick between Phantom Routing (PR) and Multi-path Routing (MR). On the other hand, the adversary can pick between Traffic Analysis (TA) and Tracing Back (TB). From the literature, the following payoff matrix (illustrated in Table 1) can be constructed. Furthermore, the average values of energy and latency presented in Table 2 can be attributed to the above routing mechanisms.

|       | TA          | TB          |
|-------|-------------|-------------|
| PR    | Long [44]   | Medium [1,10,45] |
| MR    | Medium [21] | Long [46]   |

Table 1. Survival time payoffs for the defender 2 × 2 game.

|       | PR          | MR          |
|-------|-------------|-------------|
| p     | High        | Medium      |
| q     | Long        | Medium      |

Table 2. Energy (p) and Latency (q) for each routing mechanism of the 2 × 2 game.

Clearly, the 2 × 2 game presented in Table 1 has no pure strategy Nash equilibrium. In fact, this game is similar to the famous Matching Pennies game [47], which is a cornerstone example for the notion of mixed strategy Nash equilibrium and the concept of steady state analysis of the games. Indeed, Tables 1 and 2 are not constructed from a comprehensive literature survey, and the studies in the literature may involve other parameters that may result in biased comparisons. Nevertheless, the sole purpose of Case Study-1 is to establish the following points:
• $H$, $p$, $q$ can be estimated beforehand from either simulation or emulation study of the actual networks.
• Mixed strategy Nash equilibrium is strongly applicable to the proposed defender and adversary game.

5.2. Case Study-2

The survival time payoff matrix $H$ containing the interval-based normalized survival times (values between $[0, 1]$) are given in Table 3. The normalized values in the range $[0.2, 0.4]$ may indicate short (small) survival time, latency or energy consumption, $[0.5, 0.7]$ indicates medium survival time, latency or energy consumption, and $[0.8, 1]$ indicates long survival time, latency or energy consumption. For the routing mechanisms, Table 4 presents the energy $p$ and the latency $q$ values. Suitable units for survival time, energy, and latency can be obtained from the actual network. A discussion on obtaining the above data from actual WSN is presented at the end of this section. The case study has the following key structure: The defender can change the routing policy from time to time. The defender can pick from any six routing mechanisms, say: $R_1$, $R_2$, ..., $R_6$. On the other hand, the adversary can change the attacking mechanism from time to time. The adversary can pick from any six attack mechanisms, say: $A_1$, $A_2$, ..., $A_6$.

Table 3. Survival time payoffs for the defender in Case Study-2.

|       | A1       | A2       | A3       | A4       | A5       | A6       |
|-------|----------|----------|----------|----------|----------|----------|
| $R_1$ | [0.5, 0.7] | [0.8, 1] | [0.5, 0.7] | [0.8, 1] | [0.2, 0.4] | [0.2, 0.4] |
| $R_2$ | [0.2, 0.4] | [0.5, 0.7] | [0.2, 0.4] | [0.5, 0.7] | [0.8, 1] | [0.8, 1] |
| $R_3$ | [0.5, 0.7] | [0.8, 1] | [0.8, 1] | [0.2, 0.4] | [0.5, 0.7] | [0.2, 0.4] |
| $R_4$ | [0.8, 1] | [0.2, 0.4] | [0.2, 0.4] | [0.5, 0.7] | [0.8, 1] | [0.5, 0.7] |
| $R_5$ | [0.2, 0.4] | [0.5, 0.7] | [0.5, 0.7] | [0.8, 1] | [0.2, 0.4] | [0.8, 1] |
| $R_6$ | [0.8, 1] | [0.2, 0.4] | [0.8, 1] | [0.2, 0.4] | [0.5, 0.7] | [0.5, 0.7] |

Table 4. Energy ($p$) and Latency ($q$) for each routing mechanism in Case Study-2.

|       | $R_1$ | $R_2$ | $R_3$ | $R_4$ | $R_5$ | $R_6$ |
|-------|--------|--------|--------|--------|--------|--------|
| $p$   | 0.9    | 0.7    | 0.2    | 0.6    | 0.5    | 0.3    |
| $q$   | 0.4    | 0.6    | 0.7    | 0.3    | 0.8    | 0.5    |

The grid for $\varepsilon_1$ is generated by taking 10 equally spaced intervals of $[0, 0.2 \times q_{\text{max}}]$, $[0, 0.2 \times r_{\text{max}}]$, and $[0, 0.2 \times q_{\text{max}}]$ for solving Formulations (12a–f)–(14a–f), respectively. Similarly, for $\varepsilon_2$, the grid is generated by taking 10 equally spaced intervals of $[0, 0.2 \times p_{\text{max}}]$, $[0, 0.2 \times r_{\text{max}}]$, and $[0, 0.2 \times p_{\text{max}}]$ for solving Formulations (12a–f)–(14a–f), respectively. All the models are solved using the GLPK solver (https://www.gnu.org/software/glpk/, accessed on 1 September 2022). The Pareto surface obtained after solving Formulation (12a–f) is depicted in Figure 1a, and the Pareto surfaces obtained after solving Formulations (13a–f) and (14a–f) are illustrated in blue and green colored surfaces in Figure 1b, respectively. Table 5 displays the results of the case study at $\varepsilon_1 = \varepsilon_2 = 0$, which indicates the minimax game values. From Table 5, it can be concluded that if the defender ignores the latency- and energy-related objectives, then playing $R_1$, $R_2$ or $R_6$ equally will likely be the best for LPP. Practically, it means that the network administrator can alternate between $R_1$, $R_2$ or $R_6$ to obtain the longest possible survival time, while preserving the privacy location of the sink node. Other operational points can be extracted from Figure 1b.
Figure 1. Case Study-2, Pareto surfaces. (a) Formulation (12a–f) Pareto. (b) Formulations (12a–f)–(14a–f) Pareto surfaces.

Table 5. Minimax game values (at $\varepsilon_1 = \varepsilon_2 = 0$) of Case Study-2.

|    | Optimistic | Average | Pessimistic |
|----|------------|---------|-------------|
| R1 | 0.333      | 0.333   | 0.333       |
| R2 | 0.333      | 0.333   | 0.333       |
| R3 | 0          | 0       | 0           |
| R4 | 0          | 0       | 0           |
| R5 | 0          | 0       | 0           |
| R6 | 0.333      | 0.333   | 0.333       |

5.3. Case Study-3

Case Study-3 is similar to the setup of Case Study-2. The key difference is in the data. The interval widths in Case Study-2 are constant, and the intervals are non-overlapping. In this case study, the interval widths are not constant, and the intervals are overlapping for a given row or column. The data for Case Study-3 are presented as follows: The survival time payoff matrix $H$ containing the interval-based survival times are given in Table 6, and Table 7 presents the energy $p$ and the latency $q$ values. All the models are solved using the open source GLPK solver. The Pareto surface obtained after solving Formulation (12a–f) is depicted in Figure 2a, and the Pareto surfaces obtained after solving Formulations (13a–f) and (14a–f) are illustrated in blue and green colored surfaces in Figure 2b, respectively. Table 8 displays the results of the case study at $\varepsilon_1 = \varepsilon_2 = 0$, which indicates the minimax game values. From Table 8, it can be concluded that if the defender ignores the latency- and the energy-related objectives, then, under optimistic circumstances, playing $R3$, $R5$, $R6$, $R7$ or $R8$ with the given probabilities in Table 8 is the best for LPP. In practice, this could mean that $R7$ is deployed $36.9\%$ of the time, $R3$ is deployed $26.3\%$ of the time, $R8$ is deployed $14.4\%$ of the time, and so on. Similarly, under pessimistic circumstances, playing $R1$, $R2$, $R4$, $R5$, $R6$ or $R7$ with the given probabilities in Table 8 is the best for LPP.
Table 6. Survival time payoffs for the defender in Case Study-3.

|  | A1       | A2       | A3       | A4       | A5       |
|---|----------|----------|----------|----------|----------|
| R1| [0.38, 0.83] | [0.23, 0.63] | [0.33, 0.59] | [0.09, 0.74] | [0.39, 0.99] |
| R2| [0.36, 0.81] | [0.24, 0.79] | [0.0, 0.78] | [0.39, 0.74] | [0.25, 0.5] |
| R3| [0.16, 0.91] | [0.28, 0.73] | [0.13, 0.73] | [0.0, 0.85] | [0.16, 0.56] |
| R4| [0.0, 0.61] | [0.2, 0.85] | [0.36, 0.76] | [0.33, 0.59] | [0.0, 0.59] |
| R5| [0.09, 0.95] | [0.2, 0.7] | [0.21, 0.51] | [0.30, 0.8] | [0.4, 0.8] |
| R6| [0.09 ,0.55] | [0.01, 0.91] | [0.25, 0.5] | [0.42, 0.52] | [0.10, 0.7] |
| R7| [0.11, 0.96] | [0.02, 0.62] | [0.16, 0.76] | [0.09, 0.75] | [0.38, 0.88] |
| R8| [0.0, 0.59] | [0.0, 0.89] | [0.47, 0.97] | [0.04, 0.5] | [0.33, 0.58] |

Table 7. Energy (p) and Latency (q) for each routing mechanism in Case Study-3.

|  | R1  | R2  | R3  | R4  | R5  |
|---|-----|-----|-----|-----|-----|
| p | 0.8 | 0.3 | 0.5 | 0.5 | 0.4 |
| q | 0.7 | 0.5 | 0.4 | 0.2 | 1   |

Figure 2. Case Study-3, Pareto surfaces. (a) Formulation (12a–f) Pareto. (b) Formulations (12a–f)–(14a–f) Pareto surfaces.

Table 8. Minimax game values for Case Study-3 (at $\varepsilon_1 = \varepsilon_2 = 0$).

|     | Optimistic | Average | Pessimistic |
|-----|------------|---------|-------------|
| R1  | 0          | 0.227   | 0.152       |
| R2  | 0          | 0       | 0.351       |
| R3  | 0.263      | 0       | 0           |
| R4  | 0          | 0       | 0.299       |
| R5  | 0.13       | 0.196   | 0.12        |
| R6  | 0.094      | 0       | 0.074       |
| R7  | 0.369      | 0.577   | 0.003       |
| R8  | 0.144      | 0       | 0           |
5.4. Estimating $H, p, q$

In order to implement the proposed technique, WSNs and IOTs should have flexible network design such that they can employ different routing protocols alternatively during their operations. The advancements in network softwarization could facilitate the existence of such networks. In [48], the authors surveyed the softwarization of Unmanned Aerial Vehicle (UAV) routing, while [49] presented the existing literature on AI-enabled routing protocols for UAV networks. Other applications of softwarization include, but are not limited to, Routing algorithm optimization in software-defined network Wide Area Network (WAN) [50], integrating Multi-path TCP (MPTCP), and Segment Routing (SR) paradigms over SDN/NFV [51].

Once such networks are established, $H, p, q$ can be easily obtained either by developing a simulation model or extracting empirical data from emulated networks. The simulation and emulation models should have the ability to estimate the survival times, latency, and energy for a pair of routing and attack mechanisms. Thus, for a given network under consideration, the data $H, p, q$ should be estimated via simulation model a priori by the WSN manager or the decision maker. A parametric estimation of $H, p, q$ can be a future research direction.

6. Conclusions

In this work, we present a seed for a novel direction towards designing a multi-routing Wireless Sensor Network. This approach can be argued by the fact that the adversary can choose and/or change attacking mechanisms at any given time during the time horizon. Thus, the WSN manager should have the ability to choose/alternate among different routing protocols for the longevity of the network’s LPP. Furthermore, the game theoretic model provides the WSN manager with a guide on proportion of time dedicated to each routing protocol, under optimistic, average, and pessimistic circumstances. We believe the usage of multiple routing protocols with suggested time proportions will be very effective on Location Privacy Preservation (LPP). In the future, we plan to investigate the challenges of implementing this approach in real networks and study the impact of other possible payoffs on the network performance, such as computational complexity, bandwidth utilization, and memory consumption.

Author Contributions: Conceptualization, M.N.S. and U.B.; methodology, M.N.S.; validation, M.N.S. and U.B.; resources, M.N.S. and U.B.; data curation, M.N.S.; writing—original draft preparation, M.N.S.; writing—review and editing, M.N.S. and U.B.; visualization, M.N.S.; funding acquisition, M.N.S. and U.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the Deanship of Research Oversight and Coordination (DROC) at King Fahd University of Petroleum & Minerals (KFUPM), under the grant IN171025.

Institutional Review Board Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

$D$ a set of defense mechanisms available with the defender
$A$ a set of attack mechanisms available with the adversary
$d$ a defense mechanism, where $d \in D$
$a$ an attack mechanism, where $a \in A$
$h_{d,a}$ the average survival time when the adversary picks an attack mechanism $a$ and the defender picks a defense mechanism $d$
the upper bound or optimistic value of \( h_{d,a} \)

the lower bound or pessimistic value of \( h_{d,a} \)

payoff matrix of survival times, where the \( d \)th row and \( a \)th column element is \( h_{d,a} \)

uncertain payoff matrix of survival times, where the \( d \)th row and \( a \)th column element is \( \omega_{d,a} = \left[ h_{d,a} \right] \)

a vector containing the optimistic values from the \( a \)th column of matrix \( \Omega \)

a vector containing the pessimistic values from the \( a \)th column of matrix \( \Omega \)

the expected payoff of the game, gain for the defender (loss for the adversary)

the worst expected payoff value of the defender for any arbitrary choice of \( x \)

the probability of using the mechanism \( d \) by the defender under average uncertainty conditions

vector representing probabilities of using different defense mechanisms under average uncertainty conditions, defined as \( x = [x_1, \ldots, x_D]^T \)

the probability of using the mechanism \( a \) by the adversary under average uncertainty conditions

vector representing probabilities of using different attack mechanisms under average uncertainty conditions, defined as \( y = [y_1, \ldots, y_A]^T \)

vector representing probabilities of using different defense mechanisms under optimistic uncertainty conditions

vector representing probabilities of using different defense mechanisms under pessimistic uncertainty conditions

the optimal value of \( x, \bar{x}, \) and \( 
\)

the optimal value of \( y \)

average transmission latency that can be obtained during the execution of defense mechanism \( d \)

average amount of energy that is required for implementing defense mechanism \( d \)

a vector representing transmission latency for all defense mechanisms

a vector representing energy consumption for all defense mechanisms

the expected transmission latency at operating point \( x^* \), defined as \( q_{\text{max}} = q^T x^* \)

the expected energy consumption at operating point \( x^* \), defined as \( p_{\text{max}} = p^T x^* \)

the expected energy consumption at operating points \( \bar{x}^* \) and \( x^* \), respectively, defined as \( \bar{p}_{\text{max}} = \bar{p}^T \bar{x}^* \) and \( p_{\text{max}} = p^T x^* \)

the expected transmission latency at operating points \( \bar{x}^* \) and \( x^* \), respectively, defined as \( \bar{q}_{\text{max}} = \bar{q}^T \bar{x}^* \) and \( q_{\text{max}} = q^T x^* \)

the worst payoff for the defender during average, optimistic, and pessimistic uncertainty conditions, respectively

a vector containing all ones

parameters for epsilon constraint method

References

1. Ozturk, C.; Zhang, Y.; Trappe, W. Source-location privacy in energy-constrained sensor network routing. In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington, DC, USA, 25 October 2004; pp. 88–93.

2. Afzolabi, I.; Taleb, T.; Samdanis, K.; Ksentini, A.; Flinck, H. Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions. IEEE Commun. Surv. Tutor. 2018, 20, 2429–2453. [CrossRef]

3. Cerroni, W.; Galis, A.; Shiomoto, K.; Zhani, M.F. Network Softwarization and Management. IEEE Commun. Mag. 2020, 58, 14–15. [CrossRef]

4. Tian, H.; Shen, H.; Matsuzawa, T. Randomwalk routing for wireless sensor networks. In Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT’05), Dalian, China, 5–8 December 2005; pp. 196–200.
5. Tian, H.; Shen, H.; Matsuzawa, T. Random walk routing in WSNs with regular topologies. *J. Comput. Sci. Technol.* 2006, 21, 496–502. [CrossRef]

6. Nguyen, M.T. Minimizing energy consumption in random walk routing for wireless sensor networks utilizing compressed sensing. In Proceedings of the 2013 8th International Conference on System of Systems Engineering, Maui, HI, USA, 2–6 June 2013; pp. 297–301.

7. Xi, Y.; Schwiebert, L.; Shi, W. Preserving source location privacy in monitoring-based wireless sensor networks. In Proceedings of the 20th 2006 International Parallel & Distributed Processing Symposium, Rhodes Island, Greece, 25–29 April 2006; p. 8.

8. Wang, W.P.; Chen, L.; Wang, J.X. A Source-Location Privacy Protocol in WSN Based on Locational Angle. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 1630–1634. [CrossRef]

9. Kang, L. Protecting Location Privacy in Large-Scale Wireless Sensor Networks. In Proceedings of the 2009 IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6. [CrossRef]

10. Kamat, P.; Zhang, Y.; Trappe, W.; Ozturk, C. Enhancing source-location privacy in sensor network routing. In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS’05), Columbus, OH, USA, 6–10 June 2005; pp. 599–608.

11. Kumar, P.; Singh, J.; Vishnoi, P.; Singh, M. Source location privacy using multiple-phantom nodes in WSN. In Proceedings of the TENCON 2015–2015 IEEE Region 10 Conference, Macao, China, 1–4 November 2015; pp. 1–6.

12. Sun, J.; Chen, Y.; Li, T.; Liu, J.; Yang, Y. PSSPR: A Source Location Privacy Protection Scheme Based on Sector Phantom Routing in WSNs. In Proceedings of the 2021 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Virtual Conference, 25–28 October 2021; pp. 334–340. [CrossRef]

13. Rimhjum; Roy, P.K.; Singh, J.P. Encircling the Base Station for Source Location Privacy in Wireless Sensor Networks. In Proceedings of the 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 20–22 December 2018; pp. 307–312.

14. Baroutis, N.; Younis, M. Load-conscious maximization of base-station location privacy in wireless sensor networks. *Comput. Netw.* 2017, 124, 126–139. [CrossRef]

15. Kazatzopoulos, L.; Delakouridis, C.; Marias, G.F.; Georgiadis, P. ihide: Hiding sources of information in wns. In Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU’06), Lyon, France, 29 June 2006; pp. 8–48. [CrossRef]

16. Han, G.; Xu, M.; He, Y.; Jiang, J.; Ansere, J.A.; Zhang, W. A dynamic ring-based routing scheme for source location privacy in wireless sensor networks. *Inf. Sci.* 2019, 504, 308–323. [CrossRef]

17. He, A.; Long, J.; Zhang, J. An energy-efficient multi-ring-based routing scheme for WSNs. *IEEE Access* 2019, 7, 181257–181272. [CrossRef]

18. Wang, H.; Sheng, B.; Li, Q. Privacy-aware routing in sensor networks. *Comput. Netw.* 2009, 53, 1512–1529. [CrossRef]

19. Chen, W.; Zhang, M.; Hu, G.; Tang, X.; Sangaiah, A.K. Constrained random routing mechanism for source privacy protection in WSNs. *IEEE Access* 2017, 5, 23171–23181. [CrossRef]

20. Liu, A.; Zheng, Z.; Zhang, C.; Chen, Z.; Shen, X. Secure and energy-efficient disjoint multipath routing for WSNs. *IEEE Trans. Veh. Technol.* 2012, 61, 3255–3265. [CrossRef]

21. Koh, J.Y.; Leong, D.; Peters, G.W.; Nevat, I.; Wong, W.C. Optimal privacy-preserving probabilistic routing for wireless networks. *IEEE Trans. Inf. Forensics Secur.* 2017, 12, 2105–2114. [CrossRef]

22. Huang, C.; Ma, M.; Liu, Y.; Liu, A. Preserving source location privacy for energy harvesting WSNs. *Sensors* 2017, 17, 724. [CrossRef] [PubMed]

23. Rana, S.S.; Vaidya, N.H. A new ‘Direction’ for source location privacy in wireless sensor networks’. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 342–347.

24. Das, A.; Moharana, L. Bypassing using directional transceivers: A design for anti-tracking source location privacy protection in WSNs. In Proceedings of the 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRICCN), Kolkata, India, 23–25 September 2016; pp. 39–44.

25. Dutta, N.; Saxena, A.; Chellapappan, S. Defending wireless sensor networks against adversarial localization. In Proceedings of the 2010 Eleventh International Conference on Mobile Data Management, Kansas City, MO, USA, 23–26 May 2010; pp. 336–341.

26. Nassiri, A.; Razzaque, M.A.; Abdullah, A.H. Isolated adversary zone for source location privacy in wireless sensor networks. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 108–113.

27. Freudiger, J.; Manshaei, M.H.; Hubaux, J.P.; Parkes, D.C. On non-cooperative location privacy: A game-theoretic analysis. In Proceedings of the 16th ACM conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 324–337.

28. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Baçsar, T.; Hubaux, J.P. Game theory meets network security and privacy. *ACM Comput. Surv. (CSUR)* 2013, 45, 1–39. [CrossRef]
29. Shokri, R.; Theodorakopoulos, G.; Troncoso, C.; Hubaux, J.P.; Le Boudec, J.Y. Protecting location privacy: Optimal strategy against localization attacks. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 617–627.
30. Humbert, M.; Marshalei, M.H.; Freudiger, J.; Hubaux, J.P. Tracking games in mobile networks. In Proceedings of the International Conference on Decision and Game Theory for Security, Berlin, Germany, 22-23 November 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 38–57.
31. Chen, J.; He, K.; Yuan, Q.; Xue, G.; Du, R.; Wang, L. Batch identification game model for invalid signatures in wireless mobile networks. *IEEE Trans. Mob. Comput.* 2016, 16, 1530–1543. [CrossRef]
32. Shokri, R.; Theodorakopoulos, G.; Troncoso, C. Privacy games along location traces: A game-theoretic framework for optimizing location privacy. *ACM Trans. Priv. Secur. (TOPS)* 2016, 19, 11. [CrossRef]
33. Osborne, M.J.; Rubinstein, A. *A Course in Game Theory*; MIT Press: Cambridge, MA, USA, 1994.
34. Bazaraa, M.S.; Jarvis, J.J.; Sherali, H.D. *Linear Programming and Network Flows*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
35. Harsanyi, J.C. Games with incomplete information played by “Bayesian” players, I–III Part I. The basic model. *Manag. Sci.* 1967, 14, 159–182. [CrossRef]
36. Charnes, A.; Kirby, M.J.; Raike, W.M. Zero-zero chance-constrained games. *Theory Probab. Its Appl.* 1968, 13, 628–646. [CrossRef]
37. Whinston, A.M.; Nwana, S.O.; Nwana, S.O. Solution of a satisficing model for random payoff games. *Manag. Sci.* 1972, 19, 266–271. [CrossRef]
38. Li, D.F. Linear programming approach to solve interval-valued matrix games. *Omega* 2011, 39, 655–666. [CrossRef]
39. Dey, A.; Zaman, K. A robust optimization approach for solving two-person games under interval uncertainty. *Comput. Oper. Res.* 2020, 119, 104937. [CrossRef]
40. Li, Y.; Ren, J. Source-location privacy through dynamic routing in wireless sensor networks. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
41. Tan, W.; Xu, K.; Wang, D. An anti-tracking source-location privacy protection protocol in WSNs based on path extension. *IEEE Internet Things J.* 2014, 1, 461–471. [CrossRef]
42. Wang, N.; Zeng, J. All-direction random routing for source-location privacy protecting against parasitic sensor networks. *Sensors* 2017, 17, 614. [CrossRef]
43. Owen, G. *Discrete Mathematics and Game Theory*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 1999; Volume 22.
44. Sami Oubbati, O.; Atiquzzaman, M.; Ahamed Ahanger, T.; Ibrahim, A. Softwarization of UAV Networks: A Survey of Applications and Future Trends. *IEEE Access* 2020, 8, 98073–98125. [CrossRef]
45. Rovira-Sugranes, A.; Razi, A.; Afghah, F.; Chakareski, J. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook. *Ad Hoc Netw.* 2022, 130, 102790. [CrossRef]
46. Al-Sadi, A.M.; Al-Sherbaz, A.; Xue, J.; Turner, S. Routing algorithm optimization for software defined network WAN. In Proceedings of the 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), Baghdad, Iraq, 9–10 May 2016; pp. 1–6.
47. Barakibite, A.A.; Mkwawa, I.H.; Sun, L.; Ifeachor, E. QualitySDN: Improving Video Quality using MPTCP and Segment Routing in SDN/NFV. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 182–186.