2021 17th International Conference on Mobility, Sensing and Networking (MSN) | 978-1-6654-0668-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/MSN53354.2021.00023

A robust fixed path-based routing scheme for protecting the source location privacy in WSNs

Lingling Hu, Liang Liu*, Yulei Liu, Wenbin Zhai, Xinmeng Wang
College of Computer Science and Technology
Nanjing University of Aeronautics and Astronautics
Nanjing, China
Emails: {linglinghu, liangliu, liu_yulei, wenbinzhai, WXinmeng}@nuaa.edu.cn

***Abstract*—With the development of wireless sensor networks (WSNs), WSNs have been widely used in various fields such as animal habitat detection, military surveillance, etc. This paper focuses on protecting the source location privacy (SLP) in WSNs. Existing algorithms perform poorly in non-uniform networks which are common in reality. In order to address the performance degradation problem of existing algorithms in non-uniform networks, this paper proposes a robust fixed path-based random routing scheme (RFRR), which guarantees the path diversity with certainty in non-uniform networks. In RFRR, the data packets are sent by selecting a routing path that is highly differentiated from each other, which effectively protects SLP and resists the backtracking attack. The experimental results show that RFRR increases the difficulty of the backtracking attack while safekeeping the balance between security and energy consumption.**

***Keywords*-wireless sensor network; location privacy protection; routing protocol; fixed path;**

I. Introduction

A wireless sensor network consists of a large number sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. With the development of wireless communication technique, WSNs have been widely used in many fields, such as agricultural planting, military field, medical care, animal habitat detection, emergency rescue [1], etc.

Since sensor nodes are usually deployed in unattended environments, privacy protection has become the challenge in WSNs. It is easy for the attackers to monitor nodes, steal messages, and obtain the location and sensitive data of the source node. Data privacy can be protected by encryption technology. However, due to the characteristics of WSNs' broadcast communication, the context information is exposed and the attackers can infer the location of the source node by analyzing context information without decrypting messages [2].

For example, in WSNs used to monitor the pandas' habitat, the attacker sniffs at the transmitted messages within communication range. As shown in Fig. 1, the sensor that detects the panda is the source node, and the source node transmits the panda's information to the sink through multi-hop routing. We assume that the attacker is near the sink, and sniffs at the transmitted messages within its communication range. Once a message is detected, the attacker backtracks to the location of the message sender and continues monitoring. The above process is repeated until it backtracks to the location of the source node. By the above backtracking attack, the location of the source node is traced and exposed without decrypting the message.

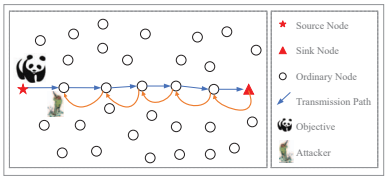


Figure 1. The backtracking attack

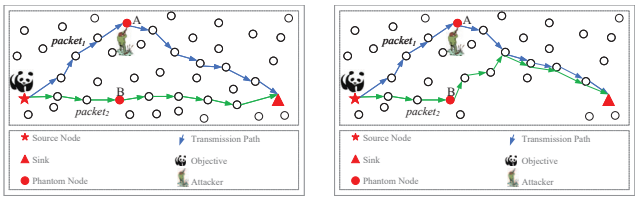
In recent years, many algorithms are proposed to protect SLP [3], [4]. Ozturk et al. first propose the concept of phantom routing [5] to protect SLP, in which each packet is first sent by the source node to a phantom node far from the source node and then sent from the phantom node to the sink. Wang et al. [6] introduce inclination angles to guide data packets to stay away from the source node. Lightfoot et al. propose a routing technique called the Sink Toroidal Region (STaR) [7], which restricts phantom nodes to a circular region to keep the phantom node at a proper distance from the source node. On the premise of tilt angle, He et al. consider balancing energy consumption and security according to the location of the source node [8].

These schemes all protect SLP by choosing the phantom node far away from the source node and extending the transmission path to confuse the attacker and hinder the backtracking attack. As shown in Fig. 2(a), two packets are sent to phantom nodes A and B that are far away from each other. When the attacker backtracks along the transmission path of $packet_1$ to the location A, it cannot continue backtracking because the source node chooses another phantom node B to forward $packet_2$ and the attacker cannot sniff to the new message $packet_2$.

These schemes works well in uniform networks, however their performance degrades in non-uniform networks. For

978-1-6654-0668-0/21/$31.00 ©2021 IEEE
DOI 10.1109/MSN53354.2021.00023

example, as shown in Fig. 2(b), the positions of the phantom nodes A and B are still far from each other in the non-uniform network. However, due to the uneven distribution of nodes, two transmission paths ($SourceNode->A->Sink$ and $SourceNode->B->Sink$) partially overlap. So the existing schemes perform poorly in the network shown Fig. 2(b). If the attacker sniffs more packets, the backtracking speed will be accelerated. So only considering the phantom node's location and the distance from the source node does not guarantee the diversity of the transmission path certainly, which cannot protect SLP well.



(a) The ordinary phantom routing (b) The problem of phantom routing

Figure 2. The phantom routing

In order to solve the above problems, this paper proposes a robust fixed path-based random routing scheme (RFRR) to ensure SLP. For each message sent by the source node to the sink, its routing path consists of two parts: the fixed path of the first N hops and the shortest path after. In each transmission, RFRR selects a new fixed path that is far enough from the previous one. It ensures transmission paths' distance between two adjacent data packets is far enough. After the fixed routing path ends, the transmission path is changed to the shortest routing path, which can reduce energy consumption while safekeeping the balance between privacy and performance. The main contributions of this paper are as follows:

- A robust fixed path-based routing scheme is proposed. By introducing the fixed path, it certainly guarantees the difference between two adjacent transmission paths. Under the premise of ensuring the diversity of paths, energy consumption is reduced as much as possible, thus ensuring SLP and trading off energy consumption and security.
- We compare the algorithm proposed in this paper with the existing classic algorithms through simulation experiments, and the results prove that RFRR is superior to existing routing schemes in terms of safe time.

The rest of this paper is organized as follows: We review the related works in Section II. Section III introduces some preliminaries. Section IV introduces our proposed scheme in detail. Section V shows and analyzes the simulation experiment results. Section VI summarizes the whole work.

II. Related work

The research of SLP was firstly led by the classic problem of "Panda Hunter Game". As shown in Fig. 1, animal protection researchers deploy a large number of sensors in Panda Nature Reserve to monitor the panda. The sensor that detects the panda is the source node, which periodically sends the monitored information to the sink. At the same time, the hunter performs the backtracking attack by monitoring data transmissions until backtracking to the position of the panda. Based on the "Panda Hunter Game", SLP in WSNs has been extensively studied.

Ozturk et al. first propose the concept of phantom routing [5] (PR) to protect SLP through phantom routing. The algorithm is divided into two stages: the random walk and the flooding stage. The algorithm diversifies the paths through the random walk phase to protect SLP. However, the flooding stage consumes lots of energy consumption.

In order to solve the problem that PR consumes too much energy, Kamat et al. propose Phantom Single-Path Routing (PSPR) based on phantom routing [5]. The packets reach the sink through the shortest path rather flooding to reduces energy consumption.

Based on PSPR, Wang et al. propose the phantom routing with locational angle (PRLA) [6]. Lightfoot et al. propose a routing technique, called the sink Toroidal Region (STaR) [7], to protect SLP. This algorithm restricts the phantom nodes to a ring area (STR) near the sink. He et al. [8] propose the idea of balancing energy consumption and security according to the location of the source node, and propose a sector-based random routing (SRR) scheme to protect SLP.

Mehta et al. introduce the global attacker model [9], in which the traffic of the entire network is collected and is used to infer the packet transmission path and the location of the source node. In order to resist it, a periodic data collection scheme is proposed to eliminate the dependence between the entire network traffic distribution and the location of the source node. However this scheme periodically sends data, which greatly increases energy consumption.

Yang et al. propose a scheme called FitProbRate (Fitted Probabilistic Rate) [10]. This scheme significantly reduces the event notification delay while keeping SLP by selecting and controlling the probabilistic distribution of message transmission intervals.

Inspired by distributed topology control, Hong et al. propose an attacker location evaluation-based fake source scheduling (FSSE) method based on stochastic processes theory [11]. It balances transmission delay and communication overhead to optimize network performance.

III. Preliminaries

A. Network model

The network model used in this paper is based on the panda-hunter model:

- n sensor nodes are deployed which can be expressed as $N = \{n_i | 1 \leq i \leq n\}$. Each sensor node is constrained by computing power and energy.
- The positions of sensor nodes remain stable after deployment. The communication radius wr of the node is limited, so every sensor node and the sink communicate through multi-hop routing.
- Each sensor node n_i can obtain its position (x_i, y_i) through GPS or positioning algorithm and the position of the sink is (x_0, y_0), where $i \in \{i | 1 \leq i \leq n\}$.
- Each sensor node shares the same secret key with the sink. It transmits the encrypted data to the sink. The attacker has no key so cannot know the contents of the encrypted data by decoding [12].

B. Attack model

In the panda-hunter model, the attacker is a hunter, and the ultimate goal is to find the source node and capture the panda by tracing packets. We assume that the characteristics of the attacker are as follows:

- The hunter is equipped with powerful and efficient radio equipment, which has unlimited energy, computing power and storage capacity.
- The hunter doesn't take any proactive actions to hinder the normal operation of WSNs, because this behavior can be easily detected by the network administrator. Therefore, the hunter only carry out passive attacks (such as eavesdropping) to determine the traffic pattern of the network [13].
- The hunter estimates the position of the sender by analysising the signal strength and moves to the estimated location quickly. As this process is repeated, the attack can perform the backtracking attack.

C. Metrics

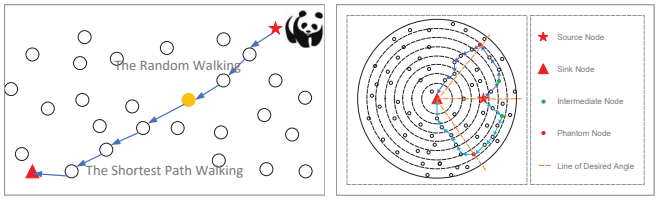
The following metrics are used to evaluate the privacy protection schemes.

- Safe time: the period that begins when the source node transmits the first data packet and ends when the attacker captures the source node [15].
- Transmission delay: the average transmission time of the data packet from the source node to the sink. It is measured by the average hop from the source node to the sink in this paper [16].
- Energy consumption: the total energy consumed by sensor nodes in WSNs. Because the energy consumed in communication is much higher than the one used to calculate, this paper only considers the former. According to [17], the energy consumption of a sensor node to send a byte of data $E_t = \alpha + \gamma \times d^n$ and the energy consumption of a sensor node to receive a byte of data $E_r = \beta$, where α represents the energy consumption of the sending circuit, γ represents the energy consumption of the transmission amplifier, d represents the transmission distance, n represents the path loss factor and β represents the energy consumption of the receiving circuit. Therefore, the energy consumed by a node $node_i$ broadcasting a byte is $E = E_t + N \times E_r$, N is the number of $node_i$'s neighbor nodes.

D. PSPR and SRR

1) PSPR: Kamat et al. propose Phantom Single-Path Routing (PSPR) [5] on the basis of phantom routing. As shown in Fig. 3(a), PSPR includes two stages. In the first stage, a data packet sent by the source node randomly walks N hops to reach the phantom node. In the second stage, this packet starts from the phantom node and reaches the sink along the shortest path. Due to the uncertainty of random walk, the transmission paths may be concentrated near the source node, it is easy for an attacker to trace back to the source node.

2) SRR: SRR divides WSNs into multiple sectors to distribute paths and protect SLP. As shown in Fig. 3(b), SRR [8] includes three stages. In the first stage, the source node calculates the random expected angle and sends a packet to the middle node further away from the sink through N hops routing. In the second stage, this packet is sent to the phantom node through the annular path routing according to the expected angle. In the third stage, this packet is sent to the sink through the shortest path routing.



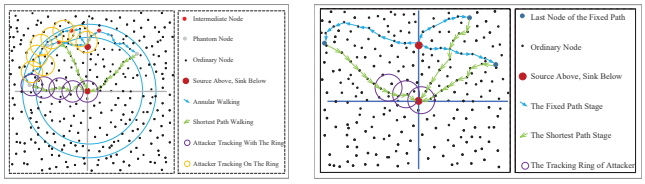
(a) PSPR (b) SRR

Figure 3. PSPR and SRR

The purpose of setting up the annular path is to disperse the paths and increases the diversity of data transmission paths. However, as shown in Fig. 4(a), because the adjacent sensors in the same ring are geographically close to each other, the speed of the attacker backtracking will be greatly accelerated once the attacker traces back to the loop area. The diversity of path is mainly reflected in the shortest path, so SRR does not guarantee the best security when the transmission delay is large. Due to the characteristics of SRR, its path is concentrated on the ring path and the inside. This also decreases partly security.

IV. RFRR

In order to solve the problem of performance degradation in non-uniform networks, this paper proposes a robust fixed path-based random routing scheme (RFRR) for protecting



(a) SRR (b) RFRR

Figure 4. The data transmission simulation of SRR and RFRR

SLP in WSNs. The symbols used in the paper are shown in Table I.

Table I
SUMMARY OF NOTATIONS

Symbol	Meaning
n_i	The sensor node i
$packet_j$	The j_{-th} packet sent by the source node
$n_i.hop$	The hop count from n_i to the sink
$n_i.shortest$	The shortest path from n_i to the sink
fp_i	The fixed path of $packet_j$ $(1 \leq i \leq M)$
$fp_i[k]$	The $(k+1)_{-th}$ node of fp_i
L	The hop count of the fixed path
bm	The beacon message
d	The half length of the shadow area
D	The distance from source to sink
n	The number of sensor nodes
$N_{circular}$	The number of circular obstacles
$R_{circular}$	The radius of circular obstacles

We assume that the source node sends a packet to the sink regularly. In order to assure the guaranteed discrimination of the fixed paths for sending different packets, M fixed paths fp_i $(1 \leq i \leq M)$ are constructed from the source node, and $packet_j$ is sent by the fixed path $fp_{j\%M}$. Our goal is to improve the diversity between $fp_{j\%M}$ and $fp_{(j+1)\%M}$, thus prolonging the safe time.

The algorithm has two stages:

- The fixed path routing: The source node transmits the packet along the fixed path that is very different than the last one.
- The shortest path routing: The last node of the fixed path sends the packet to the sink through the shortest path routing.

A. Initialization

In the initialization stage, we initialize the shortest path and the hop counts from all nodes to the sink. First, we initialize the hop counts of each node. The sink sets the hop count as $sink.hop = 0$, and the other nodes initialize the hop count to infinity (that is, the hop count from the sensor node i to the sink $n_i.hop = \infty (1 \leq i \leq n)$).

Then the sink starts broadcasting the beacon message (bm) to all neighbor nodes. The initial hop count recorded in the beacon message is 0 $(bm.hop = 0)$, and the shortest path recorded in bm is $< sink >$ $(bm.shortest =< sink >)$. Once n_i receives bm, it judge whether it meets $n_i.hop > bm.hop+1$. If it does, update n_i's and bm's shortest path to $< n_i, bm.shortest >$ and update n_i's and bm's hop count to $bm.hop + 1$. And then n_i broadcasts the updated bm to its neighbor nodes. Otherwise bm is discarded. The above processes are repeated until all nodes are completely updated [18]. The specific steps for initializing the WSN are shown in Algorithm 1.

Algorithm 1 Initialization

```
while n_i receives the bm do
    if n_i.hop > bm.hop + 1 then
        bm.hop = bm.hop + 1
        Add n_i to bm.shortest
        Update n_i.shortest to bm.shortest
        n_i.hop = bm.hop
        Broadcast bm to n_i's neighbors
    end if
end while
```

B. The construction of fixed paths

In this section, we introduce the construction algorithm of the fixed path. To ensure that the diversity of adjacent routing paths is sufficiently large, the previous fixed path fp_{i-1} needs to be considered when initializing the next fixed path fp_i. The fixed path fp_i should be as far away as possible from the previous one fp_{i-1}, so we should choose nodes that are far enough from fp_{i-1} to form fp_i.

In order to generate fixed paths, we introduce two types of messages: the generation request message and the response message of fixed path, and we refer to the two types of messages as RQ and RP respectively in the following.

As shown in Fig. 5, RQ consists of five parts: $messgType$ represents the message type ($messgType = 1$ represents RQ), i represents that the current generated is the i-th fixed path, fp_{i-1} represents the previous fixed path, $partRouting_i$ represents the partial fixed path, and $remainHop$ represents the number of remaining hops of the fixed path. In the initial RQ, $partRouting_i$ only includes the source node and $remainHop = L$ (L:The hop count of the fixed path). RP consists of three parts: $messgType$ represents the message type ($messgType = 2$ represents RP), i represents the index number of fixed path and fp_i represents the generated fixed path.

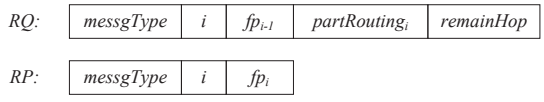


Figure 5. The request message and the response message of fixed path

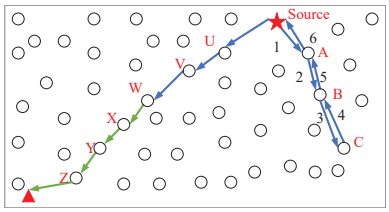


Figure 6. The setting of fixed path

We choose the former L-hop from the source's shortest path as the first fixed path. As shown in Fig. 6, we assume that $L = 3$ and the source's shortest path is $< source, U, V, W, X, Y, Z >$, so the first fixed path fp_1 is $< source, U, V, W >$. In order to ensure that the second fixed path fp_2 is far away from fp_1, fp_2 needs to be constructed based on the first one.

First, the source node generates a initial message RQ: $RQ.messgType = 1$, $RQ.i = 2$, $RQ.fp_{i-1} =< source, U, V, W >$, $RQ.partRouting_i =< source >$ and $RQ.remainHop = L$ (that is $RQ.remainHop = 3$). Then the source node selects the next-hop node of the new fixed path $RQ.fp_i$ from its neighbor nodes. Based on the number of hops, The node A farthest from $RQ.fp_{i-1}[1]$ (that is U) is used as the next-hop node. In particular, if two nodes A_1 and A_2 have the same number of hops from U, one node is randomly selected as the next hop node, the same below. The source node adds A to the $RQ.partRouting$ (that is $RQ.partRouting =< source, A >$) and subtracts $RQ.remainHop$ by one (that is $RQ.remainHop = 2$). At this time, $RQ.remainHop$ is not equal to 0, so the construction of fp_i is not over. So the source node sends RQ to A.

After A receives RQ, similarly, the node B which is farthest from $RQ.fp_{i-1}[2]$ (that is V) is selected as the next hop node. A adds B to the $RQ.partRouting$ (that is $RQ.partRouting =< source, A, B >$) and subtracts $RQ.remainHop$ by one (that is $RQ.remainHop = 1$). In the same way, $RQ.remainhop$ is not equal to 0 at this time, so A sends RQ to B. After B receives RQ, the above process is repeated: C farthest from $RQ.fp_{i-1}[3]$(that is W) is used as the next-hop node, B add C to the $RQ.partRouting$ (that is $RQ.partRouting =< source, A, B, C >$) and subtracts $RQ.remainHop$ by one (that is $RQ.remainHop = 0$). At this time, $RQ.remainhop$ is equal to 0, so the fixed path has been generated.

B needs to generate the response message of fp_i RP to transfer the new fixed path to the source node: $RP.messType = 2$ and $RP.fp_i =< source, A, B, C >$. Then B sends it to A, and A sends it to the source node, so that the second fixed path generation is over.

The subsequent fixed path generation method is the same as above, and the specific algorithm flow is shown in Algorithm 2 and 3.

Algorithm 2 The construction of fixed paths

```
while n_j receives RQ do
    k = L − remainHop
    Select the farthest node from fp_{i−1}[k] among n_j's neighbors as fp_i[k] based on the number of hops
    remainHop = remainHop − 1
    if remainHop > 0 then
        n_j sends RQ to the next-hop node
    else
        n_j generates RP
    end if
end while
```

Algorithm 3 The return of fixed paths

```
while n_j receives RP do
    Find itself fp_i[k] from fp_i
    n_j sends RP to fp_i[k − 1]
end while
```

C. Algorithm optimization

As shown in Fig. 7, when lots of fixed paths pass through the shaded area, the attacker may quickly trace backtrack to the source node, so the probability of capturing the source node will be increased. In order to prevent this problem, we set the shadow part $< Source, A_1, A_2 >$ to the invisible area of the fixed path, that is, the fixed path is not allowed to appear in this shadow area.

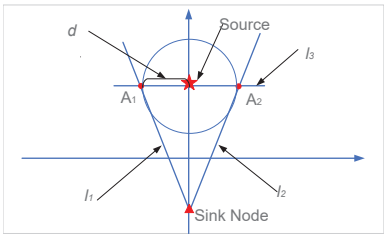


Figure 7. The straight attack

We set the shadow part to be an isosceles triangle, which is surrounded by three straight lines: $l_1 :< A_1, sink >$, $l_2 :< A_2, sink >$, $l_3 :< A_1, source, A_2 >$. The coordinates of each point are set as follows: Source: $(sourceX, sourceY)$, Sink: $(sinkX, sinkY)$, A_1: $(sourceX - d, sourceY)$, A_2: $(sourceX + d, sourceY)$.

We assume that the point on l_1 (x_1, y_1) satisfies $y_1 = k_1x_1 + b_1$, the point on l_2 (x_2, y_2) satisfies $y_2 = k_2x_2 + b_2$, and the point on l_3 (x_3, y_3) satisfies $y_3 = k_3x_3 + b_3$.

Obviously, the shaded part can be expressed by (1):

$$\begin{cases} y \geq \frac{sinkY - sourceY}{sinkX - (sourceX - d)}x + \frac{sourceY\,sinkY(sourceX - d)}{sinkX - (sourceX - d)} \\ y \geq \frac{sinkY - sourceY}{sinkX - (sourceX + d)}x + \frac{sourceY\,sinkY(sourceX + d)}{sinkX - (sourceX + d)} \\ y \leq sourceY \end{cases} \quad (1)$$

Table II
DEFAULT EXPERIMENT PARAMETERS

Parameter	Value
Network coverage area	$1000 \times 1000m^2$
Node communication radius	$50m$
Hunter listening radius	$50m$
Number of nodes	2500
Sensor data size	$50bytes$
Hops of fixed path	14
Data transmission cycle	40

However, the size of d will affect the safe time. If d is too small, the shadow area will be too small. Even if the fixed path does not pass through the shadow area, it may be caught by the attacker near the shadow area.

If d is too large, it will cause the area of the shadow part to be too large and lots of candidate domains of fixed paths will be occupied. The excessive reduction of fixed paths' candidate domain will result in the centralized distribution of fixed paths, which violates the original intention of ensuring the diversity of paths to protect SLP.

The experimental results in Section V show that the best security is achieved when $d = wr$.

V. SIMULATION

In this section, we extend the simulation model proposed by [19] to simulate PSPR, SRR and our scheme. We evaluate our scheme and compare it with PSPR [5] and SRR [8] by analyzing the impact of different parameters on the safe time, the energy consumption and the transmission delay. We conduct experiments in two different scenarios: the uniform network and the non-uniform network. The parameters under the uniform network include: the hop count of fixed path L, the size of the shadow area d, the distance from the source node to the sink D and the number of nodes n. We set up $N_{circular}$ circular obstacles with radius $R_{circular}$ in the WSN to simulate the non-uniform network. The parameters under the non-uniform network include: the number of circular obstacles $N_{circular}$ and the radius of circular obstacles $R_{circular}$. Multiple experiments are conducted and the average results are discussed.

The default parameters of the experiments are shown in Table II. The simulation experiment parameter settings of the energy consumption formula in Section III-C are shown in Table III.

Table III
ENERGY CONSUMPTION PARAMETERS [17]

Parameter	Value
γ	$10pJ/bit/m^2$
α	$45nJ/bit$
β	$135nJ/bit$
n	2

A. The impact of L

To evaluate the influence of L on RFRR, L is set from 4 to 16. The result is shown in Fig. 8. As the hop count of the fixed path L increases, both the safe time and energy consumption increase. As the hop count of the fixed path increases, the overall distance between fp_i and fp_{i-1} also increases, and the path diversity increases, which makes it more difficult for the attacker to backtrack, thereby increasing the safe time. Because energy consumption is required for each hop transmission, as the hop count of the fixed path increases, the energy consumption also increases.

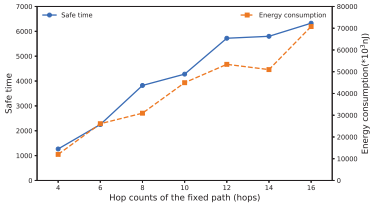
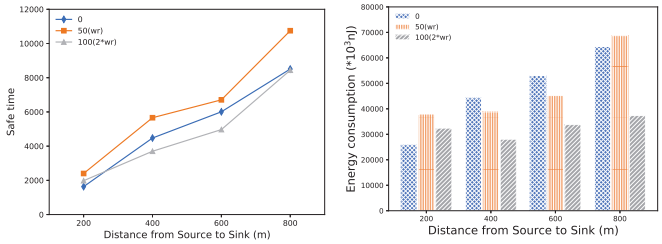


Figure 8. The safe time and energy consumption with L



(a) The safe time (b) The energy consumption

Figure 9. The safe time and the energy consumption with different d

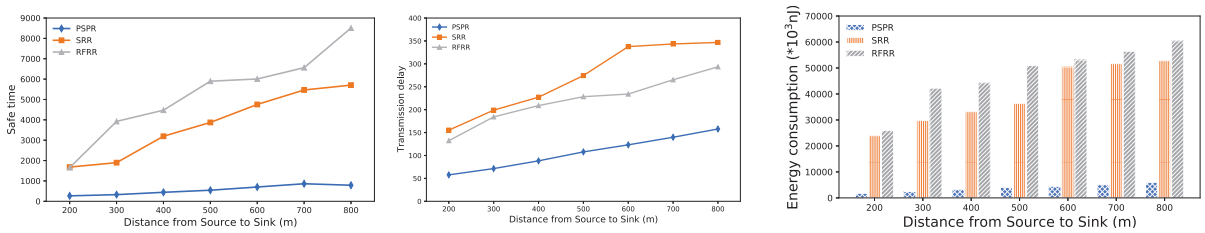
B. The impact of d

To evaluate the influence of d on RFRR, we set d from 0 to $2 \times wr$. The result is shown in Fig. 9. As shown in Fig. 9(a), d has the best security when it takes the attacker's attack radius $wr = 50$, and the security is the worst when $d = 100$. As shown in Fig. 9(b), as d increases, energy consumption decreases. The experimental results verify the analysis in Section IV-C.

C. The impact of D

To evaluate the influence of the distance from the source node to the sink, it is set from 200 to 800. The result is shown in Fig. 10.

As shown in Fig. 10(a), the safe time of PSPR, SRR and RFRR all increases as the distance from the source node to the sink increases. Because, as the distance increases, the hop counts between the source node and the sink continues



(a) The safe time (b) The transmission delay (c) The energy consumption

Figure 10. The safe time, the transmission delay and the energy consumption with different distance from Source to Sink

to increase and the path of data packet transmission continues to increase, making the backtracking hops and time of the attacker increase.

Fig. 10(b) shows the transmission delay of the three schemes. PSPR has a shorter packet transmission time and the shortest delay. SRR needs to walk through the ring path to enter the shortest path stage, and RFRR needs to pass the multi-hop fixed path to enter the shortest path stage, so they have longer transmission hops and longer delays. Simulation results show that the transmission delay of SRR is longer than that of RFRR.

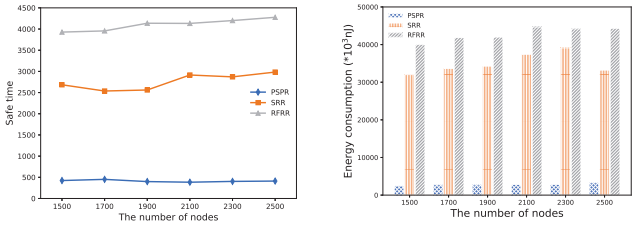
As shown in Fig. 10(c), PSPR consumes the least energy and RFRR consumes the most one. RFRR guarantees the highest safe time and more energy consumption is within the acceptable range.

According to Fig. 10(a)–10(c), the transmission delay of SRR is higher than that of RFRR, however the safe time is not, which seems unreasonable. This question has already been answered in Section III-D2. An important part of SRR is the loop path walking, and the purpose is to diversify the path and increase the diversity of the data transmission path. However, since the roaming part of the loop path is all concentrated in a ring, the attacker's traceback speed will be greatly accelerated once the attacker traces back to the loop area through the transmission path. The diversity of transmission paths is mainly reflected in the shortest path walking phase, so SRR does not guarantee the maximum safe time when the transmission delay is maximum.

At the same time, due to the characteristics of SRR, its path transmission is concentrated on the ring path and its inside. As shown in Fig. 4(b), it shows the data transmission simulation of RFRR. Due to the characteristics of RFRR's fixed path, its path transmission can be dispersed in the entire network area, the security of RFRR is improved.

D. The impact of n

As shown in Fig. 11, RFRR performs much better than PSPR and SRR in improving security. And the safe time and energy consumption of PSPR, SRR and RFRR all increase with the increase in n. Because, as n increases, the density of nodes in the WSN increases the hop counts between the source node and the sink increases under the same scale of WSNs. The hop counts between the source and the sink increases, so the time required for the attacker to backtrack increases, which result an increase of security. As shown in Section III-C, energy is mainly consumed during transmission, because the increase of the hop counts leads to an increase of energy consumption.



(a) The safe time (b) The energy consumption

Figure 11. The safe time and the energy consumption with different n

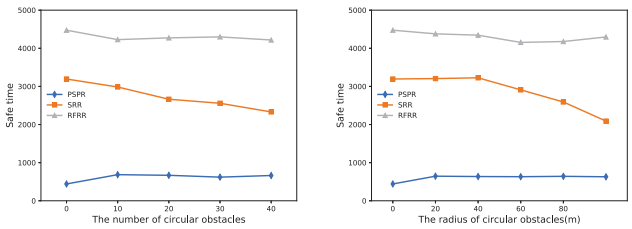
E. The impact of $N_{circular}$ and $R_{circular}$

We place obstacles in the WSN to simulate the non-uniform network. We set $N_{circular}$ circular obstacles, their radii are $R_{circular}$, any two obstacles cannot overlap, and the sensor nodes cannot be distributed within obstacles.

As shown in Fig. 12, as the obstacle radius increases or the number of obstacles increases, the irregularity of the network model increases. It can be seen that the security of SRR is decreased, while the security of RFRR has small fluctuation. Therefore, RFRR is more adaptable and robust in the non-uniform network.

VI. Conclusion

In order to solve the problem of performance degradation of existing algorithms in non-uniform networks, this paper proposes a robust fixed path-based random routing scheme (RFRR) for protecting SLP in WSNs. In RFRR, each transmission path is composed of the fixed path of the first N hops and the shortest path. Each transmission packet selects a new fixed path that is far enough from the previous path,



(a) Different number of obstacles (b) Different radius of obstacles

Figure 12. The safe time with different number of circular obstacles and different radius of circular obstacles

which ensures that the transmission path distance of two adjacent packets is far enough. After the fixed path ends, the transmission path is changed to the shortest path, which can reduce energy consumption as much as possible and balance privacy and energy consumption. The experimental results show that compared with the existing classic schemes, RFRR can guarantee higher safe time while balancing energy consumption. In a future study, we plan to explore the more secure methods to solve RFRR based on multiple source nodes.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant No.U20B2050 and the Science and Technology Funds from National State Grid Ltd.(The Research on Key Technologies of Distributed Parallel Database Storage and Processing based on Big Data).

REFERENCES

[1] T. Qiu, R. Qiao, and D. O. Wu, "Eabs: An event-aware backpressure scheduling scheme for emergency internet of things," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 72–84, 2018.

[2] B. Chakraborty, S. Verma, and K. P. Singh, "Differentially private location privacy preservation in wireless sensor networks," *Wirel. Pers. Commun.*, vol. 104, no. 1, pp. 387–406, 2019.

[3] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *2010 Proceedings IEEE INFOCOM*, 2010, pp. 1–9.

[4] G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in wsns intended for iiot," *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5527–5538, 2020.

[5] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, June 2005, pp. 599–608.

[6] W.-P. Wang, L. Chen, and J.-X. Wang, "A source-location privacy protocol in wsn based on locational angle," in *2008 IEEE International Conference on Communications*, May 2008, pp. 1630–1634.

[7] L. Lightfoot, Y. Li, and J. Ren, "Star: design and quantitative measurement of source-location privacy for wireless sensor networks," *Security Communication Networks*, vol. 9, no. 3, pp. 220–228, 2016.

[8] Y. He, G. Han, H. Wang, J. A. Ansere, and W. Zhang, "A sector-based random routing scheme for protecting the source location privacy in wsns for the internet of things," *Future Generation Computer Systems*, vol. 96, pp. 438–448, 2019.

[9] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *2007 IEEE International Conference on Network Protocols*, Oct 2007, pp. 314–323.

[10] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, April 2008, pp. 51–55.

[11] Z. Hong, R. Wang, S. Ji, and R. Beyah, "Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1337–1350, 2019.

[12] H. Li, Y. Yi, T. H. Luan, X. Liang, Z. Liang, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," *IEEE Transactions on Dependable Secure Computing*, vol. 13, no. 3, pp. 312–325, 2016.

[13] S. Mohammadi, R. E. Atani, and H. Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks," *Journal of Information Security*, vol. 2, no. 2, pp. 69–84, 2011.

[14] J. Kirton, M. Bradbury, and A. Jhumka, "Source location privacy-aware data aggregation scheduling for wireless sensor networks," in *2017 IEEE 37th International Conference on Distributed Computing Systems*, June 2017, pp. 2200–2205.

[15] J. Gui and Z. Zeng, "Joint network lifetime and delay optimization for topology control in heterogeneous wireless multi-hop networks," *Comput. Commun.*, vol. 59, pp. 24–36, 2015.

[16] A. Coman, J. Sander, and M. A. Nascimento, "Adaptive processing of historical spatial range queries in peer-to-peer sensor networks," *Distributed and Parallel Databases*, vol. 22, no. 2, pp. 133–163, 2007.

[17] M. Razzaq and S. Shin, "Fuzzy-logic dijkstra-based energy-efficient algorithm for data transmission in wsns," *Sensors*, vol. 19, no. 5, 2019.

[18] A. Coman, J. Sander, and M. A. Nascimento, "Adaptive processing of historical spatial range queries in peer-to-peer sensor networks," *Distributed Parallel Databases*, vol. 22, no. 2-3, pp. 133–163, 2007.