An Anonymous Routing Scheme for Preserving Location Privacy in Wireless Sensor Networks

Liming Zhou[1] ,Yingzi Shan[2] ,Xiaopan Chen[1]
1. School of Computer and Information Engineering, Henan University, Kaifeng 475004, China
2. Department of Finance, Yellow River Conservancy Technical Institute, Kaifeng 475004, China
lmzhou@henu.edu.cn, yzshan.yrcti@foxmail.com, xpchen@henu.edu.cn

***Abstract*—Wireless sensor networks consist of various sensors that are deployed to monitor the physical world. And many existing security schemes use traditional cryptography theory to protect message content and contextual information. However, we are concerned about location security of nodes. In this paper, we propose an anonymous routing strategy for preserving location privacy (ARPLP), which sets a proxy source node to hide the location of real source node. And the real source node randomly selects several neighbors as receivers until the packets are transmitted to the proxy source. And the proxy source is randomly selected so that the adversary finds it difficult to obtain the location information of the real source node. Meanwhile, our scheme sets a branch area around the sink, which can disturb the adversary by increasing the routing branch. According to the analysis and simulation experiments, our scheme can reduce traffic consumption and communication delay, and improve the security of source node and base station.**

Keywords—location privacy; anonymous routing; energy efficiency; wireless sensor networks

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are explored to integrate with various fields of society, so as to achieve real-time monitoring targets and transmit sensing information to base station. Although sensor nodes are limited by their own factors, such as processing capacity and power consumption, owning to the small size of sensor nodes, sensor nodes can be deployed to the monitoring area quickly. Nevertheless, WSNs are faced with many security problems, for instance sensitive information leakage, error information injection, node security authentication and many other security threats.

In wireless sensor networks, protecting location privacy is an important security issue. But the existing traditional security mechanisms cannot solve the problem of privacy disclosure. Although the adversary cannot get the content from the data packet, he can still obtain the sensitive information through other ways, such as analyzing the traffic. For instance, the adversary can observe the network traffic to get the hot spots in the network [1]. At the same time, the resource of each node in WSN is limited. When a large number of packets are transmitted among nodes, it is easy to generate unbalance energy consumption in the network. Therefore, it is necessary to develop a scheme to keep energy balance in the network.

Although many existing schemes can protect data content, they cannot effectively protect the location privacy of sensors [2-3]. The reason is that the focus issue of the research is different and many existing schemes mainly protect the data content with traditional cryptography theory. However, they cannot solve the problem of node location privacy disclosure. In addition, many schemes don't take into account the limited resource of nodes, which are easy to generate a large amount of resource consumption. Meanwhile, these schemes cannot resist the traffic analysis attack. Because data packets are transmitted among nodes and a large amount of traffic will be generated around source or sink. Therefore, when the adversary analyzes the traffic and finds the hotspot area in the network, it is easy for the adversary to gain the correct location of the source or sink and attack them. Ruan et al. [4] proposed an anonymous communication strategy, which can disturb the adversary and protect the location privacy of the real source.

In this paper, we present an anonymous routing strategy for preserving location privacy (ARPLP) in WSN. According to the remaining energy of neighbors, the source node randomly transmits a packet to several neighbor nodes with h hops and a special tag Ω. After h hops, the proxy source node with the tag Ω sends the packet to next hop. And we set a branch area around the sink to confuse the adversary. So our scheme can efficiently protect the location privacy.

The rest of the paper is organized as follow. Section 2 describes the related works. After that, Section 3 presents our anonymous routing scheme. And in Section 4 we provide simulations results of our scheme and discuss these results. Finally, we conclude this paper in Section 5.

II. RELATED WORK

Recently, location privacy has been an active area of research in wireless sensor networks. In the Random Walk scenario, each node randomly selects the next receiver until the data is sent to sink. But the packets are transmitted around the source with pure random walk. For the GROW scheme, each packet is sent to the sink following the pre-established path. But the security of sink is not considered in GROW scheme [1].

For source location privacy, Bushnag et al. [5] proposed three different techniques to protect location privacy. In order to hide the location of real source, dummy packets are injected

978-1-5386-6243-4/19/$31.00 ©2019 IEEE

in this scheme. According to balancing transmission rate of each node, three techniques can prevent the adversary from gaining the real packets. Wang et al. [6] proposed a STAMP scheme, which generates location proofs for users and protects users' privacy. Koh et al. [7] proposed an OPERA scheme, which designs a statistical decision-making framework to optimize the routing path. Meanwhile, OPERA keeps a balance between the privacy and communication cost.

Rabieh et al. [8] proposed two online fake source-based protocols, called *Dynamic* and *DynamicSPR*, to protect location privacy of real source node. In *Dynamic*, it calculate several parameters at runtime and use fake source to confuse the adversary. In *DynamicSPR,* it uses multiple fake sources to disturb the adversary and hide the accurate location of real source node. Huang et al. [9] proposed a RBCPSLP scheme that can protect source location privacy. In this scheme, RBCPSLP generates lots of routing branches in non-hotspot areas. And then, before the packets are transmitted to the sink, those routing branches are mixed into several new routing paths. Wang et al. [10] proposed a SPFP scheme, which designs a message sharing strategy to provide reliable data transmission. And this scheme uses the sharing mechanism and fake packets to hide the location of source.

For sink location privacy, Baroutis et al. [11] proposed a PLAUDIT scheme, which balances the network traffic with injecting dummy packets. So the adversary cannot find the exact location of sink. Wang et al. [12] proposed a sink location privacy preserving scheme. In this scheme, fake packets are injected into the network. This scheme uses random walk method to transmit the real packets, which is aim to hide direction information and prevent the adversary from gaining the correct direction of data transmission.

III. ANONYMOUS ROUTING SCHEME FOR PRESERVING LOCATION PRIVACY

Although many existing security techniques can protect data content, some sensitive information will still be gained by the adversary, such as the location information of nodes. Therefore, in order to preserve information of location privacy, we propose an anonymous routing strategy for preserving location privacy to address this problem.

A. Energy Model

In wireless sensor networks, when nodes receive and send data, they generate energy consumption. No matter what the routing strategy is, nodes will consume energy. Therefore, when the node sends and receives data, we only consider the energy consumption in these two aspects [13]. The transmitter sends k bits data to the receiver with the distance d and the receiver receives k bits data. So the energy consumption is given by

$$E_T(k,d)=\begin{cases} kE_{elec}+k\varepsilon_{fs}d^2, & d<d_0 \\ kE_{elec}+k\varepsilon_{amp}d^4, & d\geq d_0 \end{cases} \quad (1)$$

where E_{elec} represents the energy consumption in the transmitter or receiver circuitry. The free space (d^2 power loss) as well as the multipath fading (d^4 power loss) channel models are considered. And E_{elec} depends on the distance between transmitter and receiver. ε_{fs} and ε_{amp} are the energy required by power amplification in these two models. $E_R(k)$ indicates the energy generated by a node receiving k bits data. The energy is

$$E_R(k)=kE_{elec} \quad (2)$$

The energy parameters are shown in Table I.

TABLE I. ENERGY PARAMETERS

Parameter	Value
Initial energy (J)	2
Threshold distance $(d_0)(m)$	87
E_{elec} (nJ/bit)	50
ε_{fs} (pJ/bit/m^2)	10
ε_{amp} (pJ/bit/m^4)	0.0013

B. Protocol Description

In this section, we present an anonymous routing strategy for preserving location privacy (ARPLP) in WSN. In our scheme, the source node randomly transmits a special packet to its neighbors based on the remaining energy of neighbor nodes. And the special packet includes the number h of hops, a path queue Q and a tag Ω. When a node receives the special packet, the node must add its ID to the path queue Q. After h hops, a node receives a packet with a tag Ω, called proxy source node. Meanwhile, the proxy source node sends the path queue Q to the source. So the path in the queue is called initial path. Then the proxy source node sends the packet to next hop. The proxy source node can trap the adversary and mix up real source node making them undistinguishable to the adversary. And the base station broadcasts a special message to its neighbors which are marked by a tag Ψ. So the interference area is a special area which includes several marked nodes around the base station, called branch area.

After deploying the sensor network, each node builds its own neighbor table and energy table. The neighbor table records its all neighbors' ID. And the energy table records the remaining energy of its neighbors and itself. And the packet i includes content, hops, tag and a queue Q_i. The queue Q_i records the initial path. Firstly, the source node randomly chooses a given number of neighbors and sets the number h of hops, tag Ω and Q_i. Then the source node randomly transmits a packet to several neighbor nodes with h hops. Among them, one of selected neighbor is in the queue Q_i. If the current node is not in the queue Q_i, it will randomly transmit the packet to the next node. On the contrary, If the current node is in the queue Q_i, it will select the next node according to the initial path. After h hops, the proxy source node receives and sends the packet to next hop. Then the

packets are randomly transmitted to the next node until they reach the branch area. Meanwhile, when a node in the branch area receives a packet, it will randomly send the packet to several neighbors which is in branch area and set a tag Ψ and the number of hops. Finally, the base station receive the packet with a tag Ψ. Figure 1 illustrates the basic idea of the anonymous routing scheme.

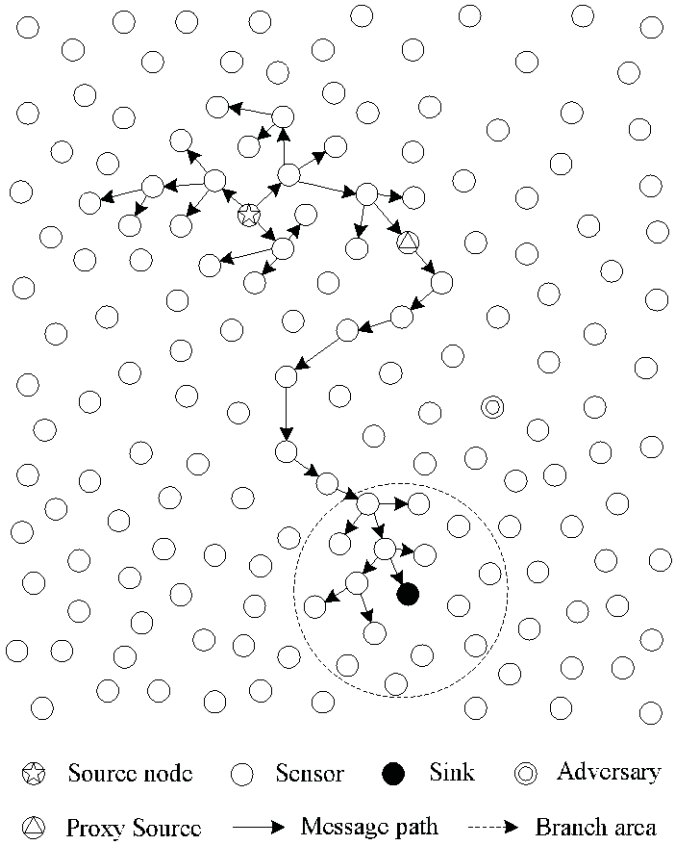

Fig. 1. The anonymous routing scheme for preserving location privacy.

C. ARPLP Algorithm

In ARPLP scheme, real source randomly transmits packets to its neighbors. These neighbor nodes randomly select the next node according to the routing rules and the queue in the packets. After h hops, the packet reaches the proxy source. Then the proxy source sends the packet to next hop. When a node in the branch area receives a packet, it will randomly send the packet to several neighbors which is in branch area and set a tag Ψ and the number of hops. Finally, the base station receives the packet with a tag Ψ. The detail of ARPLP scheme is given in Algorithm 1.

According to the above description, our scheme can effectively protect the location privacy. Meanwhile, each node randomly sends packets so that it is difficult for the adversary to obtain data forwarding rules. And the proxy source node randomly transmit the packet to its neighbors, which hides the traffic of the real source. Even if the adversary captures a packet, the next packet will not be transmitted in the same way. Therefore, the adversary cannot get data transmission strategy through observation and analysis.

Algorithm 1: ARPLP Strategy

```
current_location = source;
tag = Ω;
hops;
queue = Q;
remaining_energy;
next_location = ChooseNeighbors(current_location,
                        remaining_energy, hops, tag, queue);
proxy_source_node;
branch_area;
packetInfo;
current_node;
While(next_location != sink) do
  if(hops > 0) then
    RandomMoveTo(next_location, packetInfo, hops, tag,
queue);
  else
    RandomMoveTo(next_location, packetInfo, 0, tag,
queue);
  end if
  if(current_location in branch_area) then
    tag = SetTag( Ψ );
    hops = SetHops(remaining_energy);
    if(hops > 0) then
      RandomMoveTo(next_location, packetInfo, hops, tag,
queue);
    end if
  end if
  next_location = ChooseNeighbors(current_location,
                        remaining_energy, hops, tag, queue);
end while
```

IV. EVALUATION

In this section, we use simulations based on TOSSIM [14] to compare the performance of Random Walk and GROW with our method ARPLP in terms of latency and communication cost. According to simulation and analysis, our scheme ARPLP can effectively preserve the location privacy of source or sink and decrease the communication overhead.

In the simulation, we deploy 1,600 sensor nodes in a square area of 100×100 meters. For each sensor node, the transmission range is 2.5 meters. And an object moves in the senor network and generates real event messages. Meanwhile, the sensor nodes collect and transmit event messages to the sink.

Figure 2 shows the impact of different number of message packets to the average latency in three methods. We set the maximum latency 150 seconds. The sensors randomly choose

the next hop so that we select the average latency. For Random Walk, the packets tend to stay around the source node so that the packets are not transmitted to the base station in the maximum latency. For ARPLP and GROW, the average latency of ARPLP increases much slower compared to the GROW scheme. And the packets can be quickly sent to the base station.

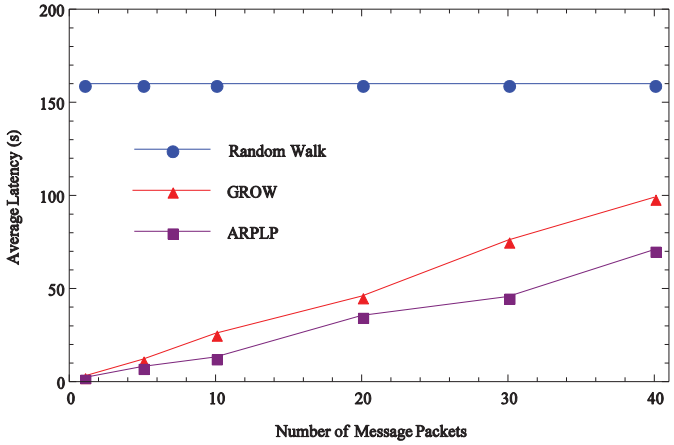

Fig. 2. The latency.

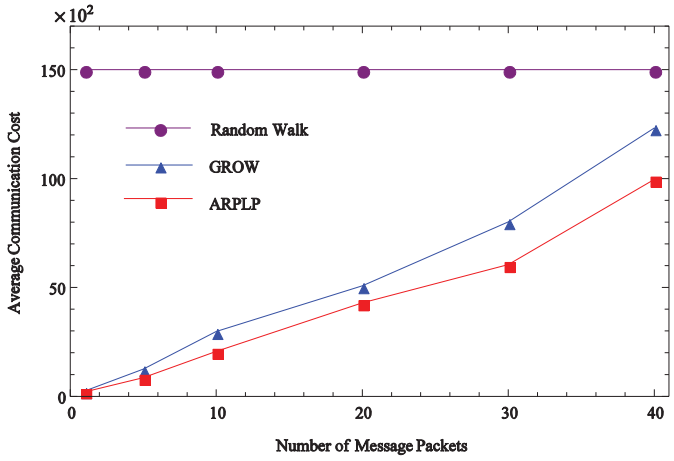

Fig. 3. The communication cost.

From Figure 3, when the packets increase, the average communication cost increases. We set the maximum communication cost 15000. For Random Walk scheme, the packets waste a large number of communication cost. However, the communication cost of ARPLP increases much slower compared to the GROW scheme. When the packets increase, the overhead obviously decreases in our method.

V. CONCLUSIONS

With the wide application of wireless sensor network, it also faces many security problems. And location privacy protection is a significant security problem. For sensitive information in sensor network, we propose an anonymous routing scheme for preserving location privacy (ARPLP) to prevent an adversary from analyzing the traffic to find the critical nodes. Our simulation and analysis show that ARPLP can hamper and interfere with the adversary's analysis and judgement. Meanwhile, the ARPLP scheme can effectively improve the security of source and sink. Then, we will continue to study lower energy consumption and safer routing strategy, so as to better protect location privacy.

ACKNOWLEDGMENT

This work is supported by NSFC (Grant No. 61402015), the Science and Technology Development Plan Project of Henan Province (Grant No. 172102210189), the Research Fund Project of Henan University (Grant No. 2016YBZR019).

REFERENCES

[1] L. Zhou, Q. Wen, "Providing location privacy against a global adversary in wireless sensor networks," Journal of Information and Computational Science, vol.10, no.15, pp.5043-5053, 2013.

[2] P. Kamat, Y.Y. Zhang, W. Trappe, C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," in ICDCS 2005: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, pp. 599-608, 2005.

[3] B. Karp, H.T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in MobiCom'00: Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 243-254, 2000.

[4] Z. Ruan, W. Liang, D. Sun, H. Luo and F. Cheng, "An efficient and lightweight source privacy protecting scheme for sensor networks using group knowledge," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 601462, 14 pages, 2013.

[5] A. Bushnag, A. Abuzneid, A. Mahmood, "Source anonymity in WSNs against global adversary utilizing low transmission rates with delay constraints," Sensors, vol.16, no.7, pp.1-17, 2016.

[6] X. Wang, A. Pande, J. Zhu, et al., "STAMP: Enabling privacy-preserving location proofs for mobile users," IEEE-ACM Transactions on Networking, vol.24, no.6, pp.3276-3289, 2016.

[7] J. Koh, D. Leong, G. Peters, et al., "Optimal privacy-preserving probabilistic routing for wireless networks," IEEE Transactions On Information Forensics and Security, vol.12, no.9, pp.2105-2114, 2017.

[8] M. Bradbury, A. Jhumka, M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," Journal of Parallel and Distributed Computing, vol.115, pp.67-81, 2018.

[9] C. Huang, M. Ma, Y. Liu, et al., "Preserving Source Location Privacy for Energy Harvesting WSNs," Sensors, vol.17, no.4, pp.1-32, 2017.

[10] N. Wang, J. Fu, J. Zeng, et al., "Source-location privacy full protection in wireless sensor networks," Information Sciences, vol.444, pp.105-121, 2018.

[11] N. Baroutis and M. Younis, "Load-conscious maximization of base-station location privacy in wireless sensor networks," Computer Networks, vol.124, pp.126-139, 2017.

[12] J. Wang, F. Wang, Z. Cao, et al., "Sink location privacy protection under direction attack in wireless sensor networks," Wireless Networks, vol.23, no.2, pp.579-591, 2017.

[13] J. Ren, Y. Zhang, and K. Liu, "An energy-efficient cyclic diversionary routing strategy against global eavesdroppers in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 834245, 15 pages, 2013.

[14] P. Levis, N. Lee, M. Welsh, D. Culler, "Tossim: Accu-rate and scalable simulation of entire tinyos applications," in SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems, pp. 126-137, 2003.