International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Novel Routing Scheme to Conceal Location Privacy in Wireless Sensor Networks

Sujay Gangaraju[1], Vamshi Krishna A[2], Paneeth Krishna A B[3], Varun Kumar E[4], Venkatesh K M[5]

[1]*Student, Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*
[2]*Student, Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*
[3]*Student, Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*
[4]*Student, Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*
[5]*Assistant Professor, Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*

Abstract - *Wireless sensor networks comprise various sensors that are deployed to watch the physical world. and lots of existing security schemes use traditional cryptography theory to safeguard message content and contextual information. However, we are concerned about location security of nodes. In this proposed paper, we are proposing an anonymous routing strategy for preserving location privacy (ARPLP), which sets a proxy source node to cover existing location of real source node. and also the real source node randomly selects several neighbours as receivers until the packets are transmitted to the proxy source. and also the proxy source is randomly selected in order that the adversary finds it difficult to get the placement information of the important source node. Meanwhile, our scheme sets a branch area round the sink, which may disturb the adversary by increasing the routing branch. Consistent with the analysis and simulation experiments, our scheme can reduce traffic consumption and communication delay, and improve the protection of source nodes and base station.*

Key Words*: *anonymous routing strategy for preserving location privacy (ARPLP), proxy source node,sink, source node, location security.

1. INTRODUCTION

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

In wireless sensor networks, protecting location privacy is a vital security issue. But the prevailing traditional security mechanisms cannot solve the matter of privacy disclosure. Wireless sensor networks (WSN) are deployed for several applications like tracking and monitoring of species, military applications, etc. which require anonymity of the origin, referred to as Source Location Privacy (SLP). The aim in SLP is to forestall unauthorized observers from tracing the source of a true event by analyzing the traffic within the network. Previous approaches to SLP like Fortified Anonymous Communication Protocol (FACP) employ transmission of real or fake packets in any time slot, which is very inefficient [1]. Privacy preserving routing protocols in wireless networks frequently make use of additional artificial traffic to hide the identities of communicating source-destination pairs. Usually, the addition of artificial traffic is done heuristically with no guarantees that the transmission cost, latency etc. are optimized in every network topology [2].

The focus of the research is different from the other papers as the many previously existing schemes mainly involve in the protection of the data content by making use of the traditional cryptographic theory. But they cannot solve the node location privacy disclosure problem. In addition, many schemes don't take into account that the resources of nodes are limited, that it is easy to generate a large amount of resource consumption. However, these schemes cannot resist the traffic analysis attack. Because data packets are transmitted among nodes and a large amount of traffic congestion 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.

In this paper, we present a unique strategy that is an anonymous routing strategy for preserving location privacy (ARPLP) in Wireless Sensor Networks. In this strategy the source node randomly transmits a packet to several neighbor nodes with h hops and a special tag. After h hops, the proxy source node bearing the tag forwards the packet to the next hop. And we set a branch area around

the sink to make the adversary stumped. So our scheme can efficiently protect the location privacy.

2. RELATED WORKS

Many of the works have been carried out on Wireless Sensor Networks based on strategies for eliminating traffic congestion and securing the message path by using various security protocols.

Wireless sensor networks (WSN) are used for various applications like tracking and monitoring of species, military applications, etc. which need anonymity of the origin, called Source Location Privacy (SLP). The aim in SLP is to restrict unauthorized observers from tracing the source of a true event by analyzing the traffic within the network. Previous approaches to SLP like Fortified Anonymous Communication Protocol (FACP) employ transmission of real or fake packets in whenever slot, which is inefficient. To beat this shortcoming, we developed three different techniques presented during this paper [1].

In this paper, we explicitly check the privacy- utility trade off problem for wireless networks and generate a novel privacy-preserving routing algorithm called optimal privacy enhancing routing algorithm (OPERA). OPERA uses a statistics based decision-making framework inorder to make the privacy of the routing protocol optimized given a utility (or cost) constraint [2].

Wireless sensor networks (WSNs) will form the building blocks of the many novel applications like asset monitoring. These applications will need to guarantee that the placement of the occurrence of specific events is kept private from attackers, in what's called the source location privacy (SLP) problem. Fake sources are utilized in numerous techniques, however, the solution's efficiency is often achieved by fine-tuning parameters at compile time. This is often undesirable as WSN conditions may change. In this paper, we first introduce an SLP algorithm – Dynamic – which estimates the relevant parameters at runtime and provides a high level of SLP, albeit at the expense of a high number of messages. To handle this, we offer a hybrid online algorithm – DynamicSPR – that uses directed random walks for the fake sources allocation strategy to decrease energy usage. We perform simulations of the varied protocols we present and our results show that DynamicSPR provides an identical level of SLP as when parameters are optimised at compile-time, with a lower number of messages sent [3].

Securing source-location privacy plays a key role in some wireless sensor network (WSN) applications. in this paper, a redundancy branch convergence-based preserved source location privacy scheme (RBCPSLP) is proposed for energy harvesting sensor networks, with the subsequent advantages: numerous routing branches are created in non-hotspot areas with abundant energy, those routing branches can merge into some routing paths before they reach the hotspot areas [4].

In this paper, a scheme called Source-location Privacy Full Protection (SPFP) is proposed. We consider a more practical adversarial model — a wise adversary — which may be a combination of world and native models. To defend against the new adversary, first, we design a light-weight message sharing scheme that's supported congruence equations. Second, each message is mapped to a group of shares. The short lengths of the shares enable them to be processed and transmitted in an energy-efficient manner [5].

The unique role of the BS attracts adversary's attention since it will be a single point of failure for the WSN. An adversary that seeks to diminish the network utility can apply traffic analysis techniques so as to uncover the sink of all traffic (i.e., the BS) and target it with denial of service attacks. In this paper, we present a method for preserving location privacy of the BS. Our technique injects deceptive transmissions towards even the traffic density across the network and makes the BS undistinguishable [6].

To address the direction attack, we present an improved scheme supported injecting fake packets and stochastic process of real packets. During this scheme, real packets do a stochastic process to cover direction information at a special phase, fake packets are injected in intersection nodes of two or more shortest paths, which may lead adversaries to fake paths. Privacy analysis shows that our scheme contains a good performance on protecting sink location. We also examine the time taken for transmission, energy consumption and safe time by simulations [7].

3. ANONYMOUS ROUTING STRATEGY FOR PRESERVING LOCATION PRIVACY(ARPLP) SCHEME

There exist many security techniques that can protect data content. However, the adversary still manages to gain some sensitive information. For example, information about nodes. To overcome this issue we present an ARPLP scheme to address this problem.

3.1 Energy Consumption Model

When nodes receive and send data, they generate energy in wireless sensor networks. The nodes will consume Energy no matter what routing strategy you are using. Therefore, we will only consider the energy consumption

when the nodes sends and receives data[8]. The transmitter sends m bits of data to the receiver with the distance d and the receiver receives m bits data. Therefore, the energy consumption would be given as:

$E_T(m,d) = mE_e + mE_f d^2$, if $d<d_o$ or $mE_e + mE_a d^4$, if $d>=d_o$ (1)

Where,

E_e= The energy consumption in the transmitter.

d^2 = The free space (power loss).

d^4 = The multiple fading (power loss).

Here, E_e depends on the distance between transmitter and receiver. E_f and E_a are the energy required for power amplification in these nodes. $E_R(m)$ indicates the energy generated by a node receiving m bit data. The energy is:

$E_R(m) = mE_e$ (2)

The energy parameters are given in Table 1.

Table -1: Energy Parameters.

PARAMETER	VALUE
Initial energy (I)	2
Threshold distance d_o	87
E_e(nJ/bit)	50
E_f(pJ/bit/m^2)	10
E_a(pJ/bit/m^4)	0.0013

3.2 ARPLP Protocol Description

We present an Anonymous Routing strategy for Preserving Location Privacy for wireless sensor networks in this section. In this scheme, the source node is randomly transmitting a special packet to its neighbouring nodes based on the remaining energy of the neighbour nodes. The special packet includes the number of hops as H, and a path Q and a tag Ω. After a node receives the special packet, the nodes must add its ID to the path queue Q. After completion of H hops, a node receives a packet along with a tag Ω, called the proxy source node. At the same time the proxy source node sends the path queue Q to the source. So the path residing in the queue is called the initial path. After this the proxy source node sends the packet to the next hop. The proxy source acts as a trap for the adversary and mixes up real source node making it undistinguishable to the adversary. The base station broadcasts a special message to its neighbour. This special message is marked by a tag ψ. Therefore, the interference area is a special area which has several marked nodes around the base station which is called a branch area.

Initially after deploying the sensor network, each node builds its own energy table and neighbour table. The energy table records the remaining energy of the neighbours and as well as its own where as the neighbour table records all the neighbours ID. The packet j includes contents like hops, tag and a queue Q. The queue Q_j records the initial path. Primarily, the source node randomly picks a given number of neighbouring nodes and sets the number H of hops, tag Ω and Q_j. After that, the source node randomly transmits a packet to several neighbouring nodes in the queue Q_j. By any chance if the current node is not in the queue Q_j, then it will randomly transmit the packet to the next node. If the current node is in the queue Q_j, it will select the next node according to the initial path. After completion of H hops, the proxy source nod should receive and send the packet to the next hop. Then the packets are sent to the branch area. At the same time, when a node in a branch receives a packet, it will randomly send the packet to several neighbouring nodes which are in the branch area and set a tag ψ and the number of hops. Finally, the tag ψ is received by the base station.

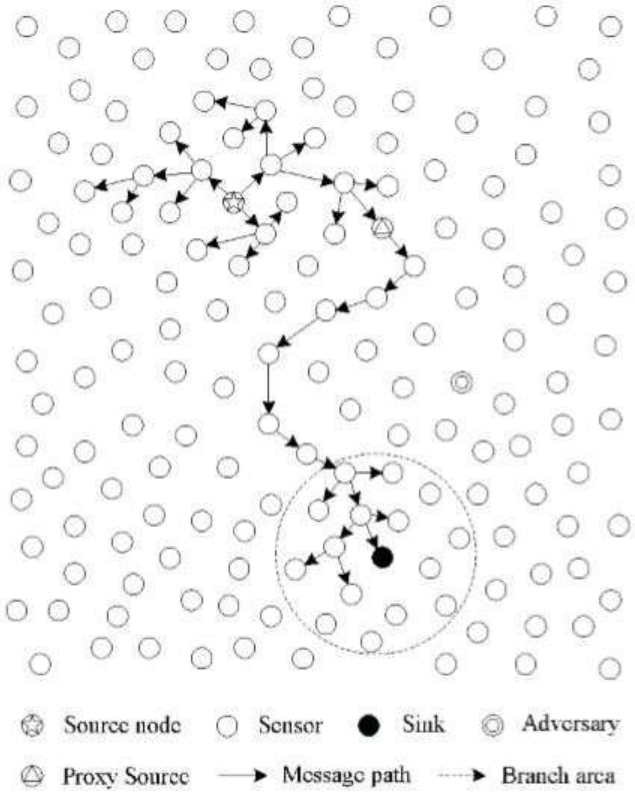

Fig -1: Demonstrates the basic idea of the anonymous routing scheme.

3.3 ARPLP Strategy Algorithm

In ARPLP strategy, packets are transmitted from the real source node to the neighbouring nodes. Each neighbouring node randomly selects a next node according to the routing rules and the queue in the packets.

```
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
```

Algorithm -1: ARPLP Algorithm.

After completing H hops, the packet reaches the proxy source node. Then the proxy source node sends the packet to the next hop. When a packet is received by a node in the branch area, it will randomly send the packet to several neighbouring nodes which are in a branch area and set a tag ψ and the number of hops. Finally, the packet is received by the base station with a tag ψ. The details of ARPLP are specified in the above Algorithm -1.

According to the description given above, our scheme can securely protect the location privacy. Meanwhile, each of the nodes randomly sends packets so that it makes it difficult to track down the data forwarding rules. The proxy source node in the meantime, randomly transmits the packet to its neighbouring nodes, which intern hides the traffic of the real source node. The adversary even if he captures a packet, the following packet will not be transmitted in the same way. Therefore, even if the adversary tries, he cannot obtain the data transmission strategy through observation and analysis.

4. EVALUATION

We use simulations based on TOSSIM[4] to compare the performance of GROW and Random Walk with the ARPLP method in terms of latency and communication cost in this section. Based on the simulations and analysis the ARPLP scheme can effectively preserve the location privacy of source or sink and decrease the communication overhead. The simulation shows the deployment of 1600 sensor nodes in a square area of 100 X 100 meters. The transmission range for each node is 2.5 meters. An object moves in the sensor network and generates real event messages, where the sensor nodes collect and transmit event messages to the sink.

The impact of different number of message packets to the average latency in these methods is shown in FIGURE II. The maximum latency is set to 150 seconds. The next hop is randomly chosen by the sensor nodes so that we select average latency. In Random Walk, the packet tends to stay around the source node so that the packets are not transmitted to the base station in maximum latency. In case of ARPLP and GROW, the average latency of ARPLP increases much slower compared to the GROW strategy. The packets can be quickly sent to the base station.

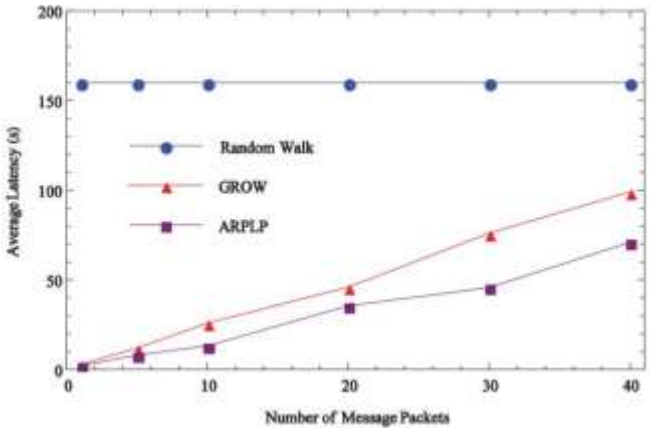

Chart -1: The Latency Test.

Chart -2 demonstrates, when the packets increase, the average communication cost increases. We need to set the maximum communication cost to 15000. In the Random Walk strategy, the packets waste a large number of communication costs. But however, the communication cost of ARPLP strategy increases much slower compared to the GROW strategy. When the packets increase, the overhead obviously decreases in the ARPLP strategy.

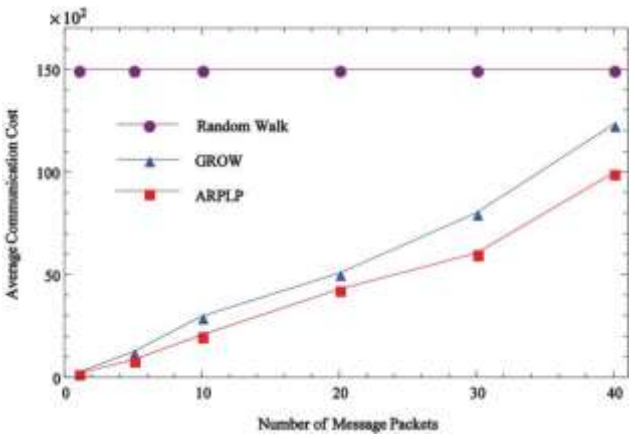

Chart -2: The Communication Cost Test.

5. CONCLUSION

There are various applications of WSN, which also face many security problems. Location privacy protection is also a significant security problem. For the preservation of sensitive information in sensor networks, we present a ARPLP strategy to safeguard and present an adversary from analysing the traffic to find the critical nodes. The simulation and analysis show that ARPLP strategy can disturb and interfere with the adversary's analysis and judgement. At the same time, the ARPLP strategy can effectively improve the security of the source and the sink nodes. Thus, we will continue to study lower energy consumption and safer routing strategy, in-order to preserve the location privacy.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Liming Zhou[1], Yingzi Shan[2], Xiaopan Chen[1], "An Anonymous Routing Scheme for Preserving Location Privacy in Wireless Sensor Networks" 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2019).