Enhancing the Location Privacy Protection Scheme in Wireless Sensor Networks

P.Bulah Pushpa Rani#1, B.Gnanakoushik #2, D.Sai Kumar #3, K.Sravan Kumar #4, A.Venkataramana #5

#1 Asst. Professor, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#2 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#3 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#4 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#5 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)

Abstract: There has been a significant use of wireless sensor networks (WSNs) for tracking valuable items. The sensor node senses in these applications the presence of artefacts and sends data packets multihop to the sink node (SN). The SN is a high-performance, efficient node which is used for gathering all of sensor node information. Because of the wireless media's open existence, an attacker can quickly follow the packet trail and find the source node. When opponents have the location of the source node, the tracked targets may be captured. It is therefore necessary to safeguard the privacy of the source node in WSNs. Many approaches have been suggested to deal with this privacy issue and most of them provide the variety of routing routes by using the fantasy node (PN), a fictional source node used to pull the opponents from the real source node. But PN is calculated in already existing schemes by the source node through floods that not only use a significant amount of overhead communication, but also shortens the source node's protection time. Considering the above problems in this article, we are proposing two new grid-based source privacy protection schemas in WSNs known as the grid-based single fantasy source node privacy protection scheme (SPS). In comparison to the node phantom in the current schemes, we suggest using a strong sink node to enable the source node to classify the PNCS, the source node chosen by random fantasy node as a false source node.

Keywords**:** wireless sensor network, privacy preservation, phantom node, random routing

I. INTRODUCTION

WIRELESS Sensor Networks (WSNs) consist of numerous sensor nodes and protocols, which is the basis of service like information authentication [1], event awareness [2], and node charging [3]. These nodes play the role of microcomputer and are distributed in various environments. There are a lot of data transmissions and communication behaviors between nodes. So, it is essential to preserve the security [4]. Security of WSNs involves many aspects, such as data privacy [5] and location privacy [6]. Data privacy can be protected by encryption algorithms while location privacy cannot be protected to the extreme.

Due to the time correlation in data transmission between two nodes, the adversary can infer location information through analysis. From a time correlation perspective, location privacy consists of the source location privacy and the sink location privacy. Given the importance of the source, in this paper, we focus on the source location privacy, which is an emerging research topic in the field of security. There are many techniques, like secure routing [7], fake sources [8], phantom nodes [9], fake cloud [10], and cluster [11], that can be applied to protect the source location privacy. We propose a probabilistic source location privacy protection scheme (PSLP), which adopts phantom nodes and fake sources for the reason that these two techniques can diversify the routing path. The steps of PSLP are as follows:

1) Phantom nodes are selected around the source and the visible area is taken into consideration.
2) A weight value, which is dynamically updated, is calculated in each node to determine the next-hop candidate.
3) Fake sources are generated around the sink to send fake packets, in order confuse the adversary. In the above steps, the visible area is a special area.

When the adversary backtracks to this area, the source can be recognized immediately. Two types of packets exist in the transmission, which are the real packets and the fake packets. Real packets are generated by the source while fake packets are generated by fake sources. In order to hide the source location, real packets sent by the source are first transmitted to a phantom node through directed random walk.

Here, considering the distance between the source and the sink, two transmission modes are taken into consideration and details will be given later. During the transmission of real packets fake packets are also transmitted to the sink with a fixed period. The proposed PSLP has exhibited a better performance than two other recent schemes in our simulations with regard to increasing the safety time while balancing the energy consumption.

The main contributions of this paper are:
1) Both phantom nodes and fake sources are integrated into the proposed PSLP, which enhance the source location privacy.
2) A more powerful local adversary, which can use Hidden Markov Model to estimate the state of the source, is taken into consideration.
3) Two data transmission modes are designed based on the distance between the source and the sink, which further enhance the source location privacy. The remainder of this paper is organized as follows.

In Section II, we provide a review of studies focused on the source location privacy. In Section III, we introduce the network and the adversary models. In Section IV, we describe the proposed PSLP in detail. In Section V, we analyze the simulation results we conclude the paper and describe planned future studies in Section VI.

II. RELATED WORK

Many researchers have paid attention to the situation privacy since Ozturk first proposed his concept [12]. Recently, location privacy has been widely researched in industrial wireless sensor networks [13], vehicular ad-hoc networks [14], cloud computing [15], and social network [16] then on.

Location privacy covers the source location privacy and therefore the sink location privacy. During this paper, we specialize in the source location privacy protection. Manjula et al. used virtual sources to protect the source location privacy [17]. In their scheme, a routing technique was proposed to maximize the security time. By adding stochastic process into the routing process, nodes in no hotspot areas participated within the establishment of multiple routing paths. Hence, the security time increased without influencing the network lifetime.

Matthew et al. proposed two algorithms using fake sources to protect the source location privacy [8]. Within the first algorithm, fake sources were dynamically deployed round the sink. Then, the sink used flooding to pick fake sources. This algorithm can provide honest source location privacy at the expense of the huge energy consumption. To deal with this, another algorithm called dynamic single path routing algorithm (DynamicSPR) was proposed. By using directed random walk, nodes far away from the source were selected as fake sources, which significantly reduced the

energy consumption. However, fake sources were related to the relative location of the source and therefore the sink, sensor nodes during a specific area might exhaust energy.

Jing et al. considered a more powerful adversary and proposed a privacy enhancing routing algorithm to guard location privacy [18]. In their research, a worldwide adversary using Bayesian maximum-a-posteriori (MAP) estimation strategy tried to watch the communication between nodes. Then, a decision-making framework was suggests to scale back the adversary's detection probability. Finally, the matter was converted into the adjustment of parameters.

Huang et al. focused on the energy utilization rate in WSNs while maintaining the source location privacy [19]. They proposed a redundancy branch-based source location privacy scheme. In their scheme, many redundancy branches were generated from the source to the sink. The amount of branches was determined by the energy collected by nodes. Additionally, these branches were converged into several routing paths later. However, the amount of converged routing paths wasn't clearly defined and therefore the energy collected by nodes round the sink might be but the energy coasted by transmitting packets.

Chen et al. in [20] proposed a constrained random walk mechanism. In their mechanism, a next-hop candidate selection domain was generated supported the offset angle of current node's neighbors and therefore the danger distance, which made the choice domain appear as if an ellipse. Then, the load of every node in the domain was calculated by the ratio between a current node's offset angle and therefore the sum of total offset angle. The smaller the ratio, the upper the probability that this node became the next hop candidate. However, the offset angle of a node was fixed, and thereby the load won't change. Thus, nodes which acted as the next-hop candidate might consume an excessive amount of energy.

Chen et al. utilized phantom nodes and proposed a limited flooding algorithm to guard the source location privacy [9]. The limited flooding was performed by the source to urge the information of nodes within the limited flooding area. Then, nodes on the sting of the limited flooding area were chosen as phantom nodes to simulate the function of the source. If a phantom node stayed behind the source, packets sent by this phantom node first bypassed the visible area and were then transmitted to the sink using the shortest path. However, the limited flooding was repeatedly performed, which could not suitable for an outsized scale network.

Li et al. in [21] proposed a scheme using random intermediate nodes and ring to guard the source location privacy. First, the authors introduced the standards to quantitatively measure the source location information leakage. Then, to scale back the leakage probability, random intermediate nodes were added to form the routing path disperse. Packets were first transmitted to an intermediate node then forwarded to a node in ring around the sink. Packets were routed on the ring for a random hop and then sent to the sink.

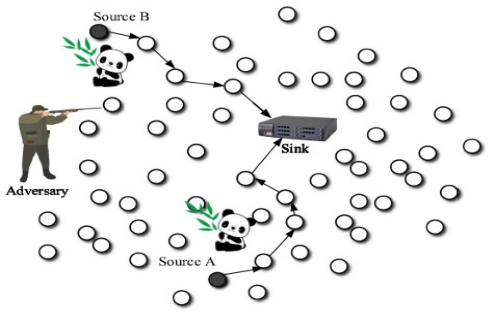


Fig. 1. The Panda-Hunter model.

To further reduce the time correlation during the transmission, Proa˜no et al.

proposed a traffic decorrelation technique to reduce the threat of a worldwide adversary [24]. The proposed traffic normalization scheme reduced the communication overhead and the transmission delay. Additionally, the entire network was partitioned into a group of minimum connected areas with a circular queue, which could reduce the active nodes during transmission and the adversary's eavesdrop probability. The privacy in their work was quantified to the space between location estimated by the adversary and therefore the location of the source.

From the above works, it are often seen that source location privacy protection has experienced an excellent improvement, techniques like fake sources, phantom nodes, stochastic process , and the weight are developed. However, these techniques are only used in a simple way, which provides us an idea.

III. MODELS AND STYLE GOALS

A. The System Model

Our system is analogous to the explanatory Panda-Hunter Game that was introduced in [11], [17]. During this Panda-Hunter Game, a sensor network is deployed to continuously monitor activities and locations of the animals during a wild animal habitat.

As soon as a panda is discovered, the corresponding source node within the nearby area will observe and report data periodically to the SINK node. However, the knowledge should be kept unavailable to the illegal hunters who may attempt to track and locate the panda. Our goal is to form it infeasible for the adversaries to determine the situation of the panda by analyzing the traffic pattern and messages transmitted through the network. We made the subsequent assumptions about our system:

- The network is evenly divided into small grids. The sensor nodes in each grid are all fully connected. In each grid, there is one header node liable for communicating with other header nodes nearby. The entire network is fully connected through multi-hop communications.
- The SINK node is that the destination location that data messages are going to be transmitted to. The knowledge of the SINK node is public. On detecting an occasion, a sensor node will generate and send messages to the SINK node through a multi-hop routing path.
- The content of every message are going to be encrypted using the shared secret key between the node/grid and therefore the SINK node. The encryption operation is beyond the scope of this paper.
- The sensor nodes are assumed to understand their relative location. We also assume that every sensor node has the knowledge of its adjacent neighboring nodes. The knowledge about the relative location of the sensor domain may also be broadcasted through this network for routing information update [18]–[20].
- The key management, including key generation, key distribution and key update, is beyond the scope of this paper. However, the interested readers are mentioned references such as [21]–[24].

B. The Adversaries Model

Due to the high profits associated with panda hunting, the adversaries would try their best to equip themselves with advanced equipments. Therefore, they typically have some technical advantages over the sensor nodes. During this paper, the adversaries are assumed to possess the subsequent characteristics:

- The adversaries will have sufficient energy resource, adequate computation capability and enough memory for data storage. On detecting an occasion, they

might determine the immediate sender by analyzing the strength and direction of the signal they received. They will move to the present sender's location without an excessive amount of delay. The adversaries can also compromise some sensor nodes within the network. We also assume that the adversaries will never miss any event when they are on the brink of the event.

- The adversaries won't interfere with the right functioning of the network, like modifying packets, altering the routing path, or destroying sensor devices, since such activities are often easily identified. However, the adversaries may perform passive attacks, like eavesdropping of the communications.
- The adversaries are ready to monitor the traffic in a neighborhood that is important to them and obtain all of the transmitted messages. However, we assume that the adversaries are unable to watch the whole network. In fact, if the adversaries could monitor the whole wireless sensor networks, then they will monitor the events directly without relying on the sensor network.

C. Design Goals

Our design goals are often summarized as followed:

- The adversaries shouldn't be ready to get the source location information by analyzing the approach pattern.
- The adversaries shouldn't be ready to get the source location information albeit they're ready to monitor certain area of the sensor network and compromise a couple of network nodes.
- Only the SINK node is in a position to spot the source location through the messages received. The recovery of the source-location from the received message should be very efficient.
- The length of every message should be as short as possible to save the previous sensor node power. This is often because that on the average, transmission of 1 bit consumes about as much power as executing 800-1000 instructions.

IV. ROUTING-BASED SOURCE LOCATION PRIVACY SCHEME

We have analyzed that phantom routing will leak direction information to the adversaries while the messages are forwarded to the phantom sources. To stop this, we proposed routing through a randomly selected intermediate node (RRIN) [22].

In this scheme, the message source first randomly selects an intermediate node at the sensor domain supported the relative location of the sensor node. The intermediate node is predicted to be distant from the important source node in order that it's difficult for the adversaries to urge the knowledge of the important source from the intermediate node selected. Since we assume that every sensor node only has knowledge of its adjacent nodes. The source node has no accurate information of the sensor nodes quite one hop away. Especially, the randomly selected intermediate node might not even exist. However, the relative location can guarantee that the message packets are going to be forwarded to the world of the intermediate node. The last node within the routing path adjacent to the intermediate

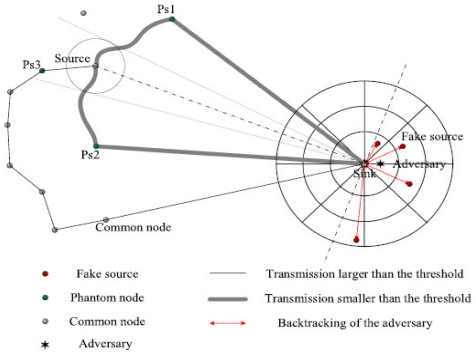


Fig. 2. Overview of PSLP.

node should be ready to tell whether such a randomly selected intermediate node

exists or not. Within the case that such a node does not exist, this node will become the intermediate node. The intermediate node then routes the received message to the destination node.

Suppose the source node is found at the relative location (x_0, y_0), to transmit a knowledge message, it first determines the minimum distance, d_{min}, that the intermediate node has got to be away from the source node. We denote the space between the source node and therefore the randomly selected intermediate node as d_{rand}. Then we've $d_{rand} \geq d_{min}$. Whenever the source node wants to get a d_{rand}, it will first generate a random number x. the worth of this random variable is generally distributed with mean 0 and variance σ2, i.e., $X \sim N(0,\sigma)$. Then the source node can calculate d_{rand} as followed:

$d_{rand} = d_{min} \times (|x| + 1)$

Therefore, the probability [27] that d_{rand} is located in the interval $[d_{min}, \rho d_{min})$ is:

$$2\varphi_{0,\sigma^2}(\rho-1)-1 = 2\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(\rho-1)^2}{2\sigma^2}}-1 = 2\varphi\left(\frac{\rho-1}{\sigma}\right)-1,$$

where ρ is a parameter larger than 1, ϕ0,σ2 is the probability density function which is the Gaussian function [28].

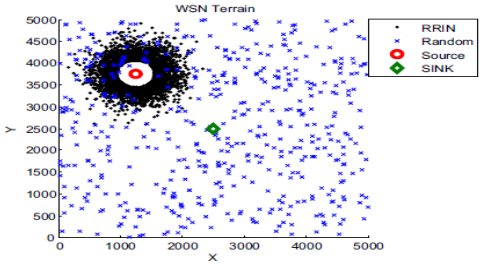


Fig. 3. Distribution of the intermediate nodes

Upon receiving data message, the intermediate node forwards the message to the SINK node.

The Determination of faux Sources As described in previous definition, fake sources are generated around the sink to extend directions from where packets come. The deployment range of a fake source is specified by angle θ_2

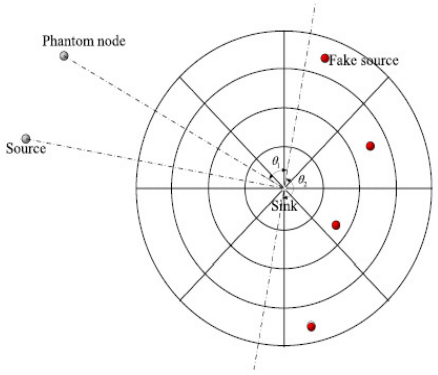


Fig. 4. Ring areas around the sink.

in Fig. 4. First of all, the sink divides the network into several rings. Then, these rings are divided into n sectors. For the sake of separating fake sources and therefore the source, fake sources are only selected within the right a part of the road which is perpendicular to the line linking the source and therefore the sink. The amount of faux sources is determined by the particular application. At the initialization, the fake source sequence is generated.

Each fake source is preferably to remain in several sectors, which guarantees that the direction of every fake packet is different. Since the adversary knows the source state during a specific time, it must analyze the packet flow to find the source. Therefore, by adopting fake sources to diversify the source location, source location privacy is protected. A node acts as a fake source for a hard and fast period. When the period of time exhausts, another fake source appears. So as to alleviate the energy consumption of fake sources, we assume that there only exists one fake source for a particular period of your time.

A. The Routing from the Source to the Sink

After the determination of phantom nodes and faux sources, the next step is that the transmission between the important source and the sink. The source transmits a message to tell the sink when it appears.

Then, the sink selects a fake source immediately after receiving this message. Considering that the source randomly appears, there exists an opportunity that distance

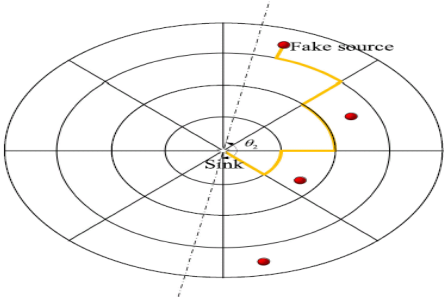


Fig. 5. Possible transmission of fake packets.

between the source and therefore the sink is little. So, in response to the present situation, we set a threshold between the source and therefore the sink. Thereby, the routing process from the source to the sink contains two scenarios. The primary case is that the hop count between the source and therefore the sink is larger than the edge. The second case is that the hop count between the source and therefore the sink is smaller than the edge. Generally, because the source first sends packets to a phantom node, the most differences dwell the choice of phantom nodes and therefore the transmission from the phantom node to the sink.

1) The Hop Count is Larger than the Threshold:

During this case, the source first routes packets to a phantom node using directed random walk. Here the choice of phantom node has no restriction due to the hop count between the source and therefore the sink is large enough. Therefore, the load is calculated by:

$$w_i = \alpha * \frac{E_{res\_i}}{E_0} + \beta * Q_i + (1 - \alpha - \beta) * \frac{H_i}{avg(\sum H_{neigbor})}$$

where E_{res_i} is that the residual energy of current node, E_0 is that the initial energy of a node, Q_i is that the communication quality per hop, which refers to the success rate of the communication transmission, Hi is that the number of hop counts from current node to the sink, and avg(Hneigbor) is that the average hop count of neighbors of current node to the sink.

2) The Hop Count is Smaller Than the Threshold:

This case is a bit complicated. Because the hop count is little, the potential candidate nodes which will be chosen as phantom nodes are limited. The source first searches nodes whose hop counts to the sink are larger than that of the source itself. These nodes should also stay outside the visible area. If no node satisfies the condition, the source selects another angular direction to pick the phantom node. Then, the source selects a phantom node from the searched nodes using directed random walk. When packets are received by the last relay node of the equal hop count routing, this node selects a next-hop candidate in its close neighbor list on the idea of the load. Since nodes around the sink may consume more energy than other nodes, weight of nodes can significantly balance the energy consumption of these nodes.

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of PSLP. All the results provided during this section are the typical values of the experimental data.

A. Overview

In this section, four metrics are evaluated within the simulation, namely, the security time, the energy consumption, the network lifetime, and therefore the transmission delay. First of all, we give the definition of each metric. The security time is that the difference between the time when the source sends the primary packet and when the adversary finds the source's location. To be more specific, we use the hop count of backtracking taken by the adversary to represent the safety time. The energy consumption represents the average energy coasted per simulation run.

PSLP is compared with two other schemes, which are the dynamic single

path routing algorithm (DynamicSPR) [8] and therefore the enhanced protocol for source location protection (SLP-E) [9]. DynamicSPR uses fake sources to guard the source location, while the SLP-E adopts phantom nodes to implement this. These

TABLE I
PARAMETER SETTINGS

Parameter	Symbol	Value
Side length	L	300-900 m
Node density	ρ	0.003 $number/m^2$
Communication radius	R	45 m
Size of a packet	l	1000 $bits$
Threshold	T	5 $hops$
Initial energy	E_0	0.5 J
Distance threshold	d_0	87 m
System parameter in the first mode	ε_{fs}	10 $pJ/bit/m^2$
System parameter in the second mode	ε_{amp}	0.0013 $pJ/bit/m^4$
Transmitting circuit loss	E_{elec}	50 nJ/bit
Data rate	v	1 $kbps$

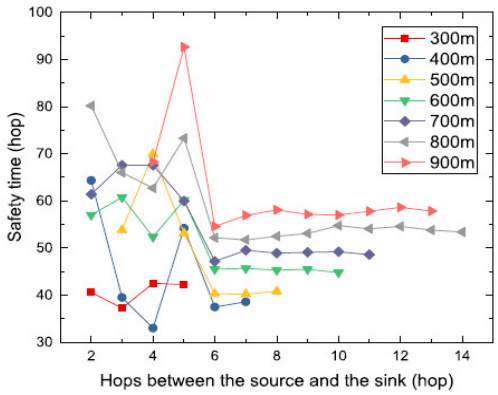


Fig. 6. Safety time versus various hops between the source and the sink.

two methods are integrated in PSLP. Therefore, we elect DynamicSPR and SLP-E for the comparison.

B. Simulation Environment and Parameter Settings

The simulation experiment is performed on MATLAB R2017b and Table I is that the parameters utilized in the simulations. Since the network size of DynamicSPR and SLP-E isn't the same, we unify the network scale within the simulation.

C. Safety Time

The longer the security time, the safer the network is. As two cases and faux sources are taken into consideration, the security time is different on each side of the edge T between the source and therefore the sink, which looks like a split point. As shown in Fig. 7, when the hop count between the source and therefore the sink is 7(which is that the pre-set threshold), there is a clear decline. This is often because the transmission of packets changes when the hop count is larger than 5.

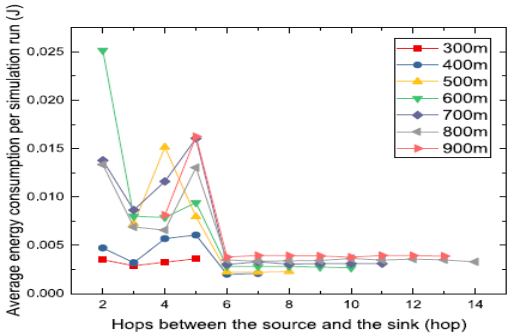


Fig. 7. Average energy consumption versus various hops between the source and the sink.

the safety time fluctuate. Additionally, the communication radius in Fig. 7 is fixed.

D. Energy Consumption

The energy consumption has an impression on the network lifetime, the less energy the node costs, the larger the network lifetime is. However, as long as increasing the security time adds extra energy consumption; a balance should be kept between the safety time and therefore the energy consumption. During this study, the energy consumption is calculated by:

$$\begin{cases} E_t = lE_{elec} + l\varepsilon_{fs}d^2 & d \le d_0 \\ E_t = lE_{elec} + l\varepsilon_{amp}d^4 & d \ge d_0 \end{cases} \quad (9)$$

$$E_r = lE_{elec} \quad (10)$$

As shown in Fig. 7, the energy consumption fluctuates with the hop count between the source and therefore the sink during a fixed communication radius. When the hop count is larger than five, nodes on the routing path are selected by the load and, therefore, the energy consumption is stabilized.

E. Network Lifetime

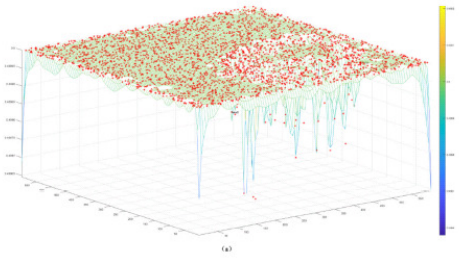
The network lifetime is influenced by many factors and therefore the energy consumption of nodes occupies an outsized proportion. As there are two transmission modes in PSLP and therefore the threshold T plays an important role during this scheme, we shall explore the connection between the network lifetime and therefore the distance between the source and therefore the sink.

F. Influence of the amount of Phantom Nodes and faux Sources

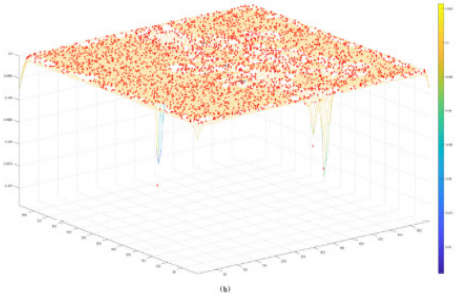
The influence of the amount of phantom nodes and faux sources on the security time and therefore the average energy consumption is shown in Fig. 8. As we will see in Fig. 8(a), the amount of phantom nodes features a little influence on the security time. This is because just one phantom node works per data transmission. Hence, the difference of the security time in each transmission is not obvious, which is merely associated with the relative position between the phantom node and therefore the source.

G. Comparison

The comparison of the transmission delay is shown in Fig. 9 and the communication radius of every node is fixed during this figure.



(a) The hop count between the source and the sink is larger than the threshold T.



(b) The hop count between the source and the sink is smaller than the threshold T.

Fig. 8. The 3-D residual energy distribution of PSLP, and the x, y, and z axes are network side length, the network side length, and the residual energy

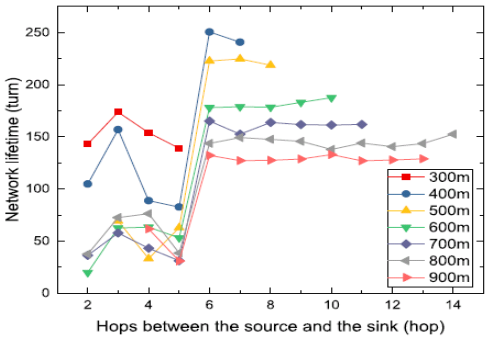


Fig. 9. Network lifetime.

We use hop because the unit of delay. The rationale is that the transmission delay is generated mainly thanks to the info TRM and the processing time, and therefore the data TRM is related to the length of routing path and therefore the rate. The data rate may be a fixed value and thus we use the unit of routing path because the unit of transmission delays.

VI. CONCLUSIONS

Studying security in WSNs became increasingly important during the last decade. In this paper, we focused on the source location privacy, a research hotspot in security, and proposed a probabilistic source location privacy protection scheme (PSLP) based on WSNs. A powerful adversary which utilizes Hidden Markov Model (HMM) is considered in this study.

To cope with it, phantom nodes, fake sources, and weight are adopted to change the packets' transmission directions. Considering the distance between the source and the sink, two types of routing modes are designed. Compared with Dynamic SPR and SLPE, the simulation results demonstrate that the proposed PSLP achieves a high safety time and balances the energy consumption of each node. Future studies will concentrate on protecting the source location by reducing the adversary's monitoring probability and secure communication among nodes.

VII. REFERENCES

[1]Rao, Mr Dr Yamarthi Narasimha, et al. "Location privacy protection in wireless sensor networks."

[2] KUMAR, P. SARAN, and Y. NARASIMHA. "Proximity Aware Data Collection in Shared Wireless Sensor Networks on Quality Monitoring." (2016).

[3] P. Golle and A. Juels, "Dining cryptographers revisited," in Advances in Cryptology - Eurocrypt 2004, LNCS 3027, pp. 456–473, 2004.

[4] S. Goel, M. Robson, M. Polte, and E. G. Sirer, "Herbivore: A Scalable and Efficient Protocol for Anonymous Communication," Tech. Rep. 2003-1890, Cornell University, Ithaca, NY, February 2003.

[5] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," IEEE J. on Selected Areas in Coomunications, Special Issue on Copyrigh and Privacy Protection, vol. 16, no. 4, pp. 482–494,1998.

[6] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for web transaction," ACM Transactions on Information and System Security, vol. 1, no. 1,pp. 66–92, 1998.

[7] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in DSN '04: Proceedings of the 2004 International Conference on Dependable Systems and Networks, (Washington, DC, USA), p. 637, IEEE Computer Society, 2004.

[8] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, pp. 113–126, Sept. 2005.

[9] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in WiSec '08: Proceedings of the first ACM conference on Wireless network security, (New York, NY, USA), pp. 77–88, ACM, 2008.

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

[11] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing sourcelocation privacy in sensor network routing," Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, pp. 599–608, June 2005.

[12] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energyconstrained sensor network routing," in SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, (New York, NY, USA), pp. 88–93, ACM, 2004.

[13] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks.," in IPDPS, IEEE, 2006.

[14] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, February 1981.

[15] D. Chaum, "The dinning cryptographer problem: Unconditional sender and recipient untraceability," Journal of Cryptology, vol. 1, no. 1, pp. 65–75, 1988.

[16] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 7, pp. 3769–3779, October 2008.

[17] http://www.panda.org/.

[18] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 829–835, April 2006.

[19] "Localization for mobile sensor networks," in MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking, (New York, NY, USA), pp. 45–57, ACM, 2004.

[20] X. Cheng, A. Thaeler, G. Xue, and D. Chen, "Tps: a time-based positioning scheme for outdoor wireless sensor networks," INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 4, pp. 2685–2696 vol.4, March 2004.

[21] H. Chan and A. Perrig, "Pike: peer intermediaries for key establishment in sensor networks," INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, pp. 524–535 vol. 1, March 2005.

[22] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," in Seventh Annual International Conference on Mobile Computing and Networks (MobiCOM 2001),
(Rome, Italy), July 2001.

[23] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T. La Porta, "Efficient hybrid security mechanisms for heterogeneous sensor networks," Mobile Computing, IEEE Transactions on, vol. 6, pp. 663–677, June 2007.

[24] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, (New York, NY, USA), pp. 62–72, ACM, 2003.

Authors Profile

P.Bulah Pushpa Rani, M.Tech., working as an Asst.Professor in the Department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.

B.Gnanakoushik pursuing B Tech in Computer Science Engineering from QIS College of Engineering and Technology (Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada.

D.Sai Kumar pursuing B Tech in Computer Science Engineering from QIS College of Engineering and Technology

(Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada.

K.Sravan Kumar pursuing B Tech in Computer Science Engineering from QIS College of Engineering and Technology (Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada.

A.Venkataramana pursuing B Tech in Computer Science Engineering from QIS College of Engineering and Technology (Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada.