Wuhan University
Journal of Natural Sciences

2016, Vol.21 No.4, 298-306

Article ID 1007-1202(2016)04-0298-09
DOI 10.1007/s11859-016-1174-5

A Novel Routing Strategy to Provide Source Location Privacy in Wireless Sensor Networks

☐ LI Shuming[1], XIAO Yan[1], LIN Qiaomin[2†], QI Zhuzhu[2]

1. Downstream Hydrology and Water Resources Survey Bureau, Yangtze River Water Conservancy Committee, Nanjing 210011, Jiangsu, China;

2. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, Jiangsu, China

Abstract: In order to secure the source location privacy when information is sent back to the base station in wireless sensor network, we propose a novel routing strategy which routes the packets to the base station through three stages: directional random routing, *h*-hop routing in the annular region and the shortest path routing. These stages provide two fold protections to prevent the source location from being tracked down by the adversary. The analysis and simulation results show that proposed scheme, besides providing longer safety period, can significantly reduce energy consumption compared with two baseline schemes.

Key words: source location privacy; wireless sensor networks (WSN); safety period; energy efficiency

CLC number: TP 393

Received date: 2015-03-04

Foundation item: Supported by the National Natural Science Foundation of China (61170065), the Natural Science Foundation of Jiangsu Province (BK20130882) and the Scientific Research Foundation of Nanjing University of Posts and Telecommunications (NY214118)

Biography: LI Shuming, male, Senior engineer, research direction: network communications and network security. E-mail: xylism@ cjh.com.cn

† To whom correspondence should be addressed. E-mail: qmlin@njupt.edu.cn

0 Introduction

The "Panda-Hunter" problem[1] is used as an application scenario for monitoring-oriented wireless sensor networks (WSN) where the location privacy is important. Different schemes have been put forward to protect the Panda's location. These schemes may be classified into many categories in which routing-based scheme is an effective way for protecting the location privacy.

The purpose of routing-based schemes is to deliver the packets in a random way through the sensor network. The random route should make a packet's path appear completely random to the adversary so as to secure the source location privacy. The randomness of the path comes from the fact that nodes deliver the packet to one of their neighbors that they choose randomly. Solutions in this category harness either a technique derived from the random walk, as described by Ozturk *et al* [2], or a technique that results in a similar pattern, such as rumor routing from Braginsky *et al* [3] and routing through randomly chose intermediate node from Li *et al* [4, 5].

Kamat *et al* [6] took the directed walk from Ozturk *et al* [2] and expanded it. A new version of the directed walk, called the hop-based directed random walk, was introduced by Kamat *et al*, which relies on the hop-distance between the sink and a node. Zhang [7] suggested that the sector-based directed random walk offered a longer safety period than the hop-base directed random walk, even though both approaches had their drawbacks.

The sector-based directed random walk is sensitive to the position where the subject is located. The hop-based

directed random walk becomes less random towards the sink, as there are less alternative paths around the sink. Zhang [7] also introduced an improvement of the sector-based directed random walk, with the introduction of the self-adjusting directed random walk. Wang *et al* [8] provided phantom routing based on the inclination angle between a node and its neighbor towards the sink. It was assumed that the adversary can be confused by choosing a random inclination angle for each packet routed from the source to the sink.

Yao and Wen [9] introduced another improvement of the random walk by combining the directed random walk. Deng *et al* [10] showed that the scheme in Ref. [9] did complicate the rate monitoring attack, but did not defend against a time correlation attack. Wang *et al* [11] mentioned that the direction information retrieved from the packet headers helped the adversary to track the source. Xi *et al* [12] provided the greedy random walk which comprised two improved random walks.

Both the random walks were improved by using a Bloom filter in the packets, to keep track of whether a node had forwarded the packet already. Xi *et al* [12] called this solution a greedy solution as it tried to cover as much of the WSN during the random walk, without creating any cycles. Lightfoot *et al* [13] argued that it was not feasible for large scale networks, and the messages leaked too much information to an eavesdropping adversary. Luo *et al* [14], inspired by several solutions, introduced a combination of three schemes to provide a stronger solution.

To the best of our knowledge, most of the solutions combine the random walk with another technique to improve the safety period. In fact, several solutions in the literature have documented weaknesses.

In this paper, it is assumed that the adversary can monitor only one local area at a time, e.g., similar to a sensor node's transmission range. A novel scheme that can provide both source location privacy and content confidentiality via a three-stage routing is proposed. In the first routing stage, the message source randomly selects a particular neighboring node in the sensor domain and then delivers the message to randomly selected neighboring node. In the second routing stage, the messages are routed in an annular region, which can dramatically increase the source location privacy. In the third routing stage, the messages will experience the shortest path routing.

The rest of the paper is organized as follows. The system model is presented in Section 1. Section 2 illustrates the specific methodology of the proposed source location privacy scheme. Then the performance evaluation is presented in Section 3. Section 3 shows the experimental results and corresponding analysis and comparison. Finally, the conclusion is arrived in Section 4.

1 System Model

The network is composed of static sensors and one base station. The terrain of our underlying network is a finite 2-dimensional grid, which is further divided into cells of equal size. Static sensors are deployed uniformly in the cells, and assumed to guarantee the connectivity of the network. All static sensors are homogeneous with the same capabilities of communication, processing, storage as well as energy. Sensor nodes communicate each other using symmetric key system. And the private key is pre-loaded into sensor node before deployment.

It is assumed that the attacker' listening radius is just the communication radius of sensor nodes. The attacker cannot tamper with or decrypt packet contents, nor destroy the sensor nodes. Initially, the attacker is in the neighborhood of base position listening communications between base station and its neighbors nodes. Once the attacker finds out that a node sends a packet to the base station, it can quickly traces to the node. During tracking process, the attacker can write down each hop. Hence it can choose to revert back to the previous node when there is no new packet's arrival for more than a certain period of time. In other words, the attacker has a strong track capability. The three-stage routing of our scheme is illustrated in Fig. 1.

Figure 1 shows two different routing path (i.e. R1 and R2) of the proposed routing technique, including three main stages. The first stage is the directional random routing which is indicated by arrow $\rightarrow$. The second stage is *h*-hop routing in the annular region that is marked by arrow $\dashrightarrow$. Finally, the data packets experience shortest path routing which is showed by arrow $\rightarrow$.

Before introduction of the proposed method, several definitions concerned are given below.

Definition 1 The neighboring node set EN: EN refers to those sensor nodes which are located in the east of some sensor and within the communication radius of that sensor.

Definition 2 The neighboring node set WN: WN refers to those sensor nodes which are located in the west of some sensor and within the communication radius of that sensor.

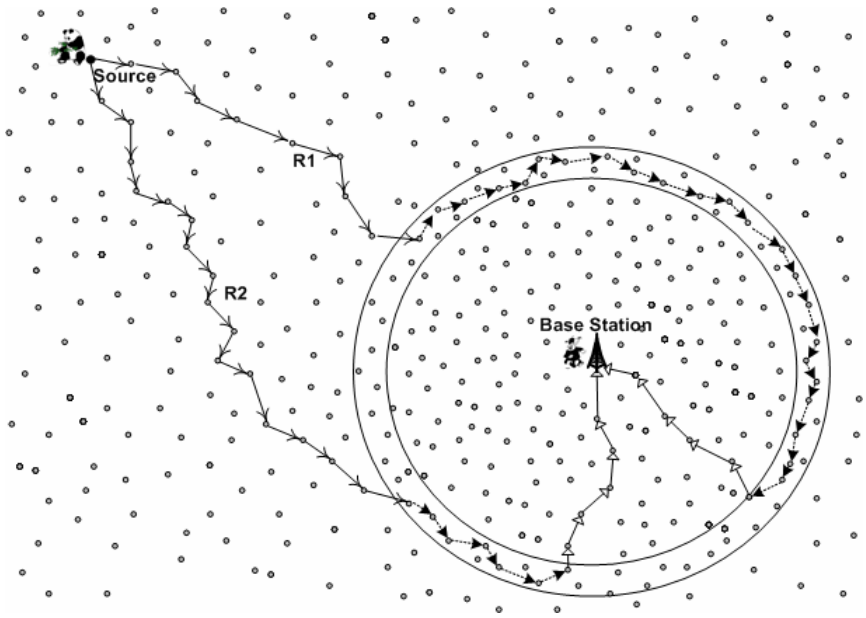

Fig. 1 Illustration of three-stage routing in proposed scheme

1-st stage routing: → 2-nd stage routing: ⇢ 3-rd stage routing: ⇨

Definition 3 The neighboring node set SN: SN refers to those sensor nodes which are located in the south of some sensor and within the communication radius of that sensor.

Definition 4 The neighboring node set NN: NN refers to those sensor nodes which are located in the north of some sensor and within the communication radius of that sensor.

Definition 5 The annular region: Provided that sensor nodes be deployed uniformly in the covered area, sensor nodes whose minimum hops to the base station range between m and n ($n \geqslant m > 0$, n and m are system parameters) are approximately round forming a ring area. The ring area is called as the annular region.

Definition 6 Random hop counts in the annular region R_h: R_h is the parameter which specifies the routing hops in the annular region. It is a random value in natural number range 1-h. Here, h is a system parameter and is assigned an integer value during system initialization. Generally, the value of h should be bigger either when n and m are bigger or when the density of sensor nodes is higher.

2 Methodology

2.1 Three-stage Routing of Proposed Scheme

The proposed scheme is described in detail as follows:

① Network initialization

Step 1: Integer system parameters n and m are initialized in the base station.

Step 2: Flood operation is initiated by the base station. The minimum hop value to the base station is recorded by each sensor node in this process. At the same time sensor node is labeled as the annular region node in case its minimum hop value to the base station is no less than m and no more than n.

Step 3: Each sensor maintains four sets for all its neighbors. EN, WN, SN and NN include respectively all neighbors in the east, west, south and north of itself. Thereby each neighbor will be included by two sets. One possible means to achieve the partition is that, after the sensor network deployment, the east-most node and the north-most node are marked. Then two floods are initiated by the two nodes to establish the relationships in east-west dimension and south-north dimension between two neighboring nodes. Each sensor stores the IDs and the minimum hops to the base station for all its neighbors. Besides, each sensor can identify whether its neighbor is in the annular region or not.

Step 4: Parameter h is initiated with an integer value.

Step 5: Each sensor records the direction of base station relative to itself in the process of flood in Step 2.

② Surveillance target

Step 6: Upon detection of target the source node

begins to generate data packets. Two binary bits called as direction bits are attached to each packet so as to indicate the direction of base station. For the first bit, 0 stands for the east direction; While 1 stands for the west direction. For the second bit, 0 stands for the south direction; And 1 stands for the north direction. Then the data packets are encrypted awaiting delivery.

Step 7: The source node selects two neighbor node sets according to direction bits: choose EN when the first bit is 0, otherwise choose WN when the first bit is 1. Similarly, choose SN while the second bit is 0 and choose NN while the second bit is 1. Then, the source node picks up randomly one neighbor node from selected two neighbor node sets as the next hop node, whose minimum hop to the base station is less than the current one. The source node delivers the encrypted packet to the next hop node.

Step 8: The packet is received by the next hop. If the next hop node is in the annular region, then turn to Step 10. Otherwise, turn to Step 9.

Step 9: The next hop node decrypts the packet and picks up randomly one neighbor node from the neighbor node sets specified by direction bits as next hop node, whose minimum hop to the base station is still less than the current one. Forward the packet to next hop node. Then turn to Step 8.

Note: Here, the first phase of the three-stage routing ends.

Step 10: The annular region node decrypts the received packet and randomly chooses one set from two corresponding neighbor node sets according to the direction bits. One binary bit is attached to the packet so as to record the selection: 0 stands for the selection of neighbor node set corresponding to the first bit of direction bits. Otherwise, 1 stands for the selection of neighbor node set corresponding to the second bit of direction bits. Then, the parameter R_h is assigned a random value within the scope 1-h (h is initialized in Step 4). And the value of R_h is added to the packet (as a hop field). Another annular region node from the chosen neighbor node set is randomly picked up as the next hop. The packet with the hop field and binary selection bit is encrypted and delivered to the next hop node.

Step 11: The annular region node decrypts the received packet and extracts the hop field value. If the value is 0 after it is reduced by 1, turn to Step 16. Otherwise, the direction bits and selection bit are also extracted to count the number of annular region nodes in the chosen neighbor node set. If the number is 0, turn to Step 13. Otherwise, turn to Step 12.

Step 12: Another annular region node from the chosen neighbor node set is randomly picked up as the next hop. The packet with updated hop value is encrypted and delivered to the next hop node. Then turn to Step 11.

Step 13: The annular region node computes the number of annular region nodes in another unchosen neighbor node set. If the number is 0, turn to Step 16. Otherwise, another annular region node from the unchosen neighbor node set is randomly picked up as the next hop. The packet with updated hop value is encrypted and delivered to the next hop node.

Step 14: The annular region node decrypts the received packet and extracts the hop field value. If the value is 0 after it is reduced by 1, turn to Step 16. Otherwise, the direction bits and selection bit are also extracted to count the number of annular region nodes in the unchosen neighbor node set. Turn to Step 16 if the number is 0. Otherwise, turn to Step 15.

Step 15: Another annular region node from the unchosen neighbor node set is randomly picked up as the next hop. The packet with updated hop value is encrypted and delivered to the next hop node. Then turn to Step 14.

Note: Here, the second phase of the three-stage routing ends.

Step 16: The annular region node chooses one neighbor node from four neighboring node sets as the next hop, whose minimum hop to the base station is the smallest. The packet without selection bit, direction bits and hop field is encrypted and delivered to the next hop node.

Step 17: The next hop node chooses one neighbor node from four neighboring node sets as the next hop, whose minimum hop to the base station is the smallest. The packet is forwarded to the next hop node.

Step 18: If the next hop node is the base station, the delivery of the packet ends and turn to Step 6. Otherwise, turn to Step 17.

There is an assumption that the private key is preloaded into the sensor nodes before deployment. And the communications between sensor nodes are encrypted using the private key. Then, the algorithm of three-stage routing can be presented as below.

Algorithm Three-stage Routing

Initialization:

(a) network initialization
(b) node initialization

(c) neighbor initialization

The source node s begins to send packets to the base station hop by hop. Each packet p experiences the following three phases.

Phase Ⅰ:

1. direction bits are attached to p=p||direction bits
2. encrypt p||direction bits=$E(p$||direction bits)
3. s randomly choose a neighboring node corresponding to the direction bits as the next hop node, whose minimum hop to the base station is less than the source node
4. s sends $E(p$||direction bits) to the next hop node
5. **while** next hop is not annular region node
   do
   next hop node decrypt $E(p$||direction bits)= p||direction bits;
   next hop node randomly choose a neighboring node corresponding to the direction bits as the next hop node, whose minimum hop to the base station is less than current one;
   forward $E(p$||direction bits) to next hop node;
   end while

Phase Ⅱ:

6. the annular region node k decrypt $E(p$||direction bits)= p||direction bits
7. k randomly chooses one set from two corresponding neighbor node sets according to the direction bits
8. selection bit is attached to p||direction bits= p||direction bits||selection bit
9. R_h is assigned a random value and attached to p||direction bits||selection bit, thus the result is p||direction bits||selection bit||R_h
10. another annular region node from the chosen neighbor node set is randomly picked up as the next hop
11. k sends $E(p$||direction bits||selection bit||R_h) to the next hop node
12. the annular region node decrypts $E(p$||direction bits||selection bit||R_h)
13. **while** (--R_h!=0)&& (the number of annular region nodes in the chosen neighbor node set is not zero)
    do
    another annular region node from the chosen neighbor node set is randomly picked up as the next hop;
    forward $E(p$||direction bits||selection bit||R_h) to next hop node;
    end while
14. **if** (R_h ==0) **then**
    go to **phase Ⅲ**
    end if
15. the annular region node j computes the number n of annular region nodes in another unchosen neighbor node set
16. **if** (n==0) **then**
    go to **Phase Ⅲ**
    end if
17. another annular region node from the unchosen neighbor node set is randomly picked up as the next hop
18. j sends $E(p$||direction bits||selection bit||R_h) to the next hop node
19. the annular region node decrypts $E(p$||direction bits||selection bit|| R_h)
20. **while** (--R_h!=0)& & (the number of annular region nodes in the unchosen neighbor node set is not zero) **do**
    another annular region node from the unchosen neighbor node set is randomly picked up as the next hop;
    forward $E(p$||direction bits||selection bit||R_h) to next hop node;
    end while

Phase Ⅲ:

21. the current annular region node decrypts $E(p$||direction bits||selection bit||R_h)
22. the current annular region node encrypts p and forwards $E(p)$ to the base station using shortest-path strategy

2.2 Analysis

The aim of the sensor network is to monitor the target, while the strategy of routing is two-fold. One is to improve the source location privacy and the other is to decrease the communication cost. The contents of all delivered packets in our scheme are encrypted by private keys. As a result, the adversary cannot acquire the contents and trace the location of sensors.

It is assumed that sensor i forwards a packet which is observed by the adversary at time t. And each observation is a tuple (i, t). Let O_T be all observations made by the adversary. We call each such set of observations as a possible trace. There is a close relationship between the analysis of location information and the source location privacy. The more confusion the adversary analyzes the location of sensors, the better protection is. It is assumed that the adversary attempts to identify a set $S_T \subset O_T$ of sensors which represent a possible trace to the source

node. Let S_P be the set of the protected sensors. Information-theoretic called entropy[15] is used to measure the privacy protection offered by proposed scheme. The entropy of tracking the source in the network can be defined as

$$e_0 = -\sum_{i=1}^{|S_T|} P_i \cdot \log_2(P_i), \tag{1}$$

Where P_i is the probability that sensor i is the source node, and $\sum_{i=1}^{|S_T|} (P_i) = 1$. Hence, the probability P_i of any nodes in S_T can be measure as $|S_P|/|S_T|$. Then the size of $|S_T|$ is denoted as $L(|S_T| = L)$. And let l be the size of the protected nodes set ($|S_P| = l$). Then the source location privacy can be defined as

$$\begin{aligned} e_1 &= -\sum_{i=1}^{|S_T|} \frac{|S_P|}{|S_T|} \cdot \log_2(\frac{|S_P|}{|S_T|}) \\ &= -\sum_{i=1}^{|S_T|} \frac{l}{L} \cdot \log_2(\frac{l}{L}) \\ &= m \cdot \log_2(\frac{l}{L}) \end{aligned} \tag{2}$$

The entropy characterizes the adversary's uncertainty about the source location. The maximum privacy can be achieved when the probabilities P_i fit uniform distribution. Let Q is the nodes set of the whole network, and $|Q| = N$, where N is the number of sensors in the whole network. Thereby, we have the optimal privacy

$$\begin{aligned} e &= -\sum_{i=1}^{|S_T|} \frac{|S_P|}{|S_T|} \cdot \log_2(\frac{|S_P|}{|S_T|}) \\ &= |S_P| \cdot \log_2(\frac{|S_T|}{|S_P|}) \\ &\leqslant m \cdot \log_2(\frac{N}{l}) \end{aligned} \tag{3}$$

We notice that source location privacy can be measure by S_P and S_T. In different cases, the privacy can be altered for different requirements. Now that the packets are delivered via different routing path which can be far from each other, it is impossible for the adversary to acquire packets continuously from a monitored sensor. What's more, even if the same packet is acquired by the adversary at different forwarding sensors, the adversary cannot infer the direction to the source by following the trace of the packets in that the packets are forwarded in a random way. Thus, it can be regarded that trace time is proportional to the trace distance and trace hop count.

To further analyze the energy efficiency of the proposed scheme, the energy model in Ref. [16] is harnessed. To transmit a k-bit data to a distance d, the radio expends energy:

$$\begin{aligned} E_{\mathrm{TX}}(k,d) &= E_{\mathrm{TX\text{-}elec}}(k) + E_{\mathrm{TX\text{-}amp}}(k,d) \\ &= \begin{cases} E_{\mathrm{elec}}k + k\varepsilon_{\mathrm{fs}}d^2, d < d_0 \\ E_{\mathrm{elec}}k + k\varepsilon_{\mathrm{mp}}d^4, d \geqslant d_0 \end{cases} \end{aligned} \tag{4}$$

$E_{\mathrm{TX\text{-}elec}}(k)$ denotes the energy consumption of radio dissipation, while $E_{\mathrm{TX\text{-}amp}}(k,d)$ denotes the energy consumption for amplifying radio. Depending on the distance between transmitter and receiver, both the free space $\varepsilon_{\mathrm{fs}}$ (d^2 power loss) and the multi-path fading $\varepsilon_{\mathrm{mp}}$ (d^4 power loss) channel models are used. When receiving this data, the radio expends energy

$$E_{\mathrm{RX}}(k) = E_{\mathrm{RX\text{-}elec}}(k) = E_{\mathrm{elec}}k \tag{5}$$

Here, the energy consumption at the receiver end can be denoted as

$$\begin{aligned} \mathrm{Cost} &= \sum_{i=1}^{N} E_{\mathrm{RX}}(k_i) \\ &= E_{\mathrm{elec}} \sum_{i=1}^{N} k_i \end{aligned} \tag{6}$$

3 Performance Evaluation

In this section, simulations are conducted to compare PR scheme (phantom routing scheme [6]), CR scheme (credit routing scheme[17]) and the proposed one. These schemes are implemented on TOSSIM[18] and evaluated based on two metrics: safety period and energy consumption. In the simulations, 10 000 sensors are deployed uniformly at random in a 1 000 1 000 m^2 area. It is assumed that the base station is located at the center of this field. Each sensor can communicate with other sensors in a radius of 30 m. We noticed that, on average, the number of neighbors for a node is 15. During the simulations, it is assumed that there is only one adversary with detection range of 30 m. The adversary always begins tracing from the base station. Once a message transmission is detected, the adversary immediately moves to the location of the transmitting node and waits for the next detection. The experiment is repeated 10 times with different network topologies and all the re-

sults were obtained by computing the average of all corresponding results.

3.1 Safety Period

The strategy for the adversary is to start from the base station and backtrack the last hop when he/she overhears a packet. Since each packet from the source node follows a different random path, it is very hard for the adversary to reliably catch a packet.

Even if he/she stays at one location and eventually overhears a packet, the last hop of the packet might be at some location he/she has already visited at each time the packet follows a random path. In such a case, the adversary obtains no new information and makes no progress towards the source node. To verify that the proposed three-stage routing scheme will not lead the adversary to the source node, a backtracking algorithm corresponding to the routing scheme is implemented to simulate the adversary.

We first investigate the impact of the parameters n, m and h on the safety period in proposed scheme. Supposed that the packet delivering interval of the source node is 0.1 s, the impact of the parameters n, m and h on the safety period of our proposed scheme can be illustrated in Fig. 2.

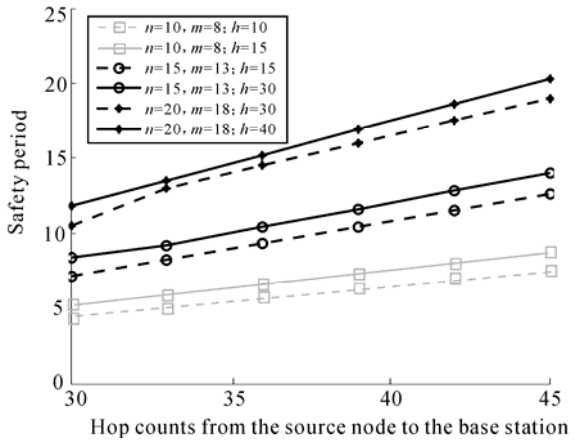

Fig. 2 Safety periods of proposed scheme

Figure 2 shows the safety periods of proposed scheme in six different cases. It is obvious that safety periods become longer in all cases as the hop counts from the source node to the base station get bigger. The reason is simple: the bigger the hop counts from source to base station is, the longer the routing path from source to base station is, which in turn, increases the difficulty of backtracking for the adversary.

According to the methodology of proposed scheme, bigger n and m mean bigger annular region, i.e. the routing paths from the source to the base station are more diversified and confusing. As a result, it can be seen in Fig. 2 that the safety period is longer when n and m are assigned bigger values. In other words, source location privacy is in proportion to the value of n and m. What needs to be pointed out is that bigger value of n and m also means more energy consumption. Hence, there is a trade-off between source location privacy and energy consumption.

We also noticed that the parameter of h has direct impact on the safety period: bigger h, longer safety period. For example, in case of n=10, m=8, the safety period when h is 15 is longer than that when h is 10. It is also the case when n=15, m=13 and n=20, m=18. This phenomenon can be explained as bigger h makes the second phase of routing more diversified. As a result, the adversary has more difficulty in backtracking.

Two backtracking algorithms corresponding to the other two routing schemes are also implemented for comparison among these three routing schemes.

Figure 3 shows the safety periods of the source location privacy of all three routing schemes. It is obvious that the proposed scheme achieves the highest safety period in the case of n=15, m=13, h=30 and n=20, m=18, h=30 and n=20, m=18, h=40. In these three cases the safety periods of proposed scheme increase rapidly as the hop count increases. Besides, we notice that the safety period of PR scheme is longer than that of our proposed scheme in the case of n=15, m=13, h=15 when hop count is below 39.

However, when the hop count is larger than 39, the safety period of proposed scheme in the case of n=15, m=13, h=15 gets longer than that of PR scheme, as indicates that proposed scheme is more competitive in terms

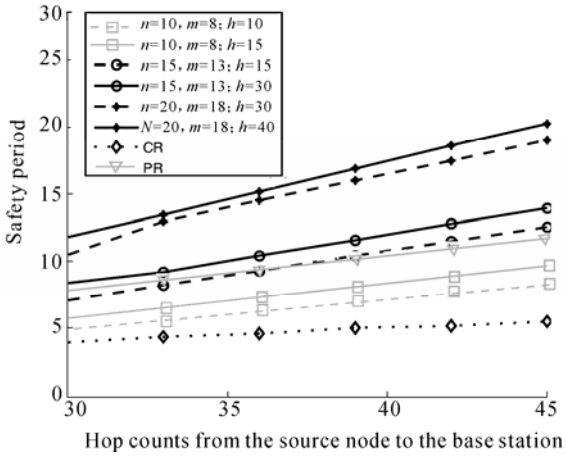

Fig. 3 Safety periods of three routing schemes

of safety period as the network scale gets larger. The safety period of CR scheme is relatively low. Obviously, the proposed scheme outperforms the CR scheme in all cases.

3.2 Energy Consumption

Generally, packet transmission is the most energy consuming operation in wireless sensor networks. Packet reception also consumes considerable energy, often on the same magnitude as packet transmission. Other power consumption aspects of delivering a packet from the source node to the base station are omitted for simplicity. Hence the simulation comparison is done based on the total number of routing hops.

All these three routing schemes improve source location privacy by scattering the packets' delivery into zigzag routing paths. Hence the packets in these three schemes travel more hops and thereby consume more energy compared with packet routing in the greedy shortest-path routing normally used in wireless sensor networks. Here, the energy overhead is investigated for all these three privacy-aware routing protocols.

In that the overhead of power consumption is proportional to the number of hops in the routing path according to equation (6), $r = h_a / h$ is denoted as the energy consumption ratio of the privacy-aware routing protocol to shortest path routing, where h_a is the average number of hops in routing paths of the privacy-aware schemes, and h is the minimum hops between the base station and the source node.

Ten times simulations are run for PR, CR and proposed scheme. The source node delivers 3 000 packets to the base station in each simulation. The average hops and present corresponding energy consumption ratio are recorded in Fig. 4.

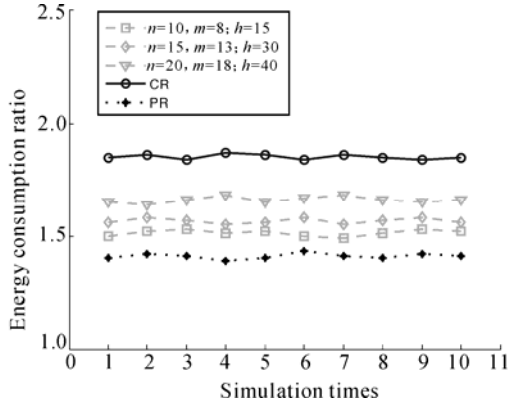

Fig. 4 Energy consumption of the routing schemes

It is not a surprise to see all three privacy-aware routing protocols consume more energy than the shortest-path approach. What surprises us is CR has the largest energy consumption ratio, while its safety period is shorter than both of the others (as can be seen from Fig. 3). The reason can be explained as follows. In CR, every intermediate node randomly and equally chooses one of its neighboring nodes (which have a smaller number of hops to the base station) as the next hop node, hence the next hop node may not be the one (among the neighbors) that is closest to the base station. As a result, the packet delivery efficiency could be poor in that it may cost several hops to forward a packet which otherwise could be directly routed in just a single hop.

In comparison, the energy overhead in PR is the lowest among all three privacy-aware routing schemes. At first glance, PR seems more promising because of its merit of low energy consumption. Nevertheless, according to the discussion of Ref. [10], PR is not recommended for practical application since once the delivered packet is captured on the random walk path, the adversary will be able to get the direction information stored in the header of the packet. As a result, the exposure of direction information decreases the complexity for adversary to trace back to the actual source node.

The proposed scheme demands more energy consumption and needs approximately 50% over the shortest path scheme in the case of n=10, m=8, h=15. Nevertheless, the extra energy consumption of proposed scheme is the trade-off for source location privacy. Accounting for the longer safety period depicted in Fig. 3, it can be believed that around 50% energy consumption is a worthwhile sacrifice for source location privacy.

4 Conclusion

Source location privacy is most crucial to the successful deployment of WSN for many applications. In this paper, we introduce a scheme that can provide source location privacy in WSN via a three-stage routing: the directional random routing, the h-hop routing in the annular region and the shortest path routing. Performance evaluation, conducted using TOSSIM, shows that the proposed scheme enjoys the longest safety period as the hop count is larger than 39. Besides, it also achieves the best trade-off between energy consumption and source location privacy. Both theoretical and simulation results indicate, in comparable scenarios, the proposed scheme is more promising than two baseline routing-based schemes in terms of safety period and energy consumption.

References

[1] Hu R H, Dong X M, Wang D L. Protecting data source location privacy in wireless sensor networks against a global eavesdropper[EB/OL].[2014-08-13]. *http*: *//downloads. hindawi.com/journals/ijdsn/*2014/492802*.pdf.*

[2] Ozturk C, Zhang Y, Trappe W. Source-location privacy in energy-constrained sensor network routing [C] // *Proc* 2*nd ACM Work-shop on Security of Ad Hoc and Sensor Networks*. New York: ACM Press, 2004: 88-93.

[3] Braginsky D, Estrin D. Rumor routing algorithm for sensor networks [C] // *Proc* 1*st ACM International Workshop on Wireless Sensor Networks and Applications*. New York: ACM Press, 2002: 22-31.

[4] Li Y, Ren J. Providing source-location privacy in wireless sensor networks [C] // *Proc International Conference on Wireless Algorithms*, *Systems and Applications*. Berlin: Springer-Verlag, 2009: 338-347.

[5] Li Y, Lightfoot L, Ren J. Routing-based source-location privacy protection in wireless sensor networks [C] // *Proc IEEE International Conference on Electro/Information Technology*. Piscataway: IEEE Press, 2009: 29-34.

[6] Kamat P, Zhang Y, Trappe W. Enhancing source-location privacy in sensor network routing [C] // *Proc* 25*th IEEE International Conference on Distributed Computing Systems*. Los Alamitos: IEEE Press, 2005: 599-608.

[7] Zhang L. A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing [C] // *Proc* 2006 *International Conference on Wireless Communications and Mobile Computing*. New York: ACM Press, 2006: 33-38.

[8] Wang W P, Chen L, Wang J X. A source-location privacy protocol in WSN based on locational angle [C] // *Proc IEEE International Conference on Communications*. Piscataway: IEEE Press, 2008: 1630-1634.

[9] Yao J, Wen G. Preserving source-location privacy in energy-constrained wireless sensor networks [C] // *Proc* 28*th International Conference on Distributed Computing Systems*. Los Alamitos: IEEE Press, 2008: 412-416.

[10] Deng J, Han R, Mishra S. Counter measures against traffic analysis attacks in wireless sensor networks [C] // *Proc First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. Washington D C: IEEE Press, 2005: 113-126.

[11] Wang H, Hsiang T. Defending traffic analysis with communication cycles in wireless sensor networks [C] // *Proc* 10*th International Symposium on Pervasive Systems*, *Algorithms*, *and Networks*. Washington D C: IEEE Press, 2009: 166-171.

[12] Xi Y, Schwiebert L, Shi W. Preserving source location privacy in monitoring-based wireless sensor networks [C] // *Proc* 20*th International Parallel and Distributed Processing Symposium*. Piscataway: IEEE Press, 2006: 425.

[13] Lightfoot L, Li Y, Ren J. Preserving source-location privacy in wireless sensor network using star routing [C] // *Proc* 2010 *IEEE Global Telecommunications Conference*. Piscataway: IEEE Press, 2010: 1-5.

[14] Luo X, Ji X, Park M. Location privacy against traffic analysis attacks in wireless sensor networks [C] // *Proc International Conference on Information Science and Applications*. Piscataway: IEEE Press, 2010: 1-6.

[15] Mahmoud M, Shen X. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks [J]. *IEEE Transactions on Parallel and Distributed Systems*, 2012, **23**(10): 1805-1818.

[16] Lin Q M, Yang J W, *et al*. Distributed face recognition in wireless sensor networks[EB/OL]. [2014-05-19]. *http*: //*downloads.hindawi.com/journals/ijdsn/*2014/175864*. pdf.*

[17] Lu Z, Wen Y. Credit routing for source-location privacy protection in wireless sensor networks [C] // *Proc IEEE* 9*th International Conference on Mobile Adhoc and Sensor Systems*. Las Vegas: IEEE Press, 2012: 164-172.

[18] Abderrazak A, Tarek M. TOSSIM and distributed binary consensus algorithm in wireless sensor networks [J]. *Journal of Network and Computer Applications*, 2014, **41**: 451-458.

□