Intelligent Silent Zone for Source-Location Privacy Based on Context-Awareness in WSNs

Zhou Qian[1,2], *Qin Xiaolin*[1*], *Ding Youwei*[1,2]

1. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, P. R. China;
2. Jiangsu Key Laboratory of Internet of Things and Control Technology, Nanjing 211106, P. R. China

(Received 18 June 2017; revised 20 November 2017; accepted 20 November 2017)

Abstract: In many wireless sensor networks (WSNs) applications, the preservation of source-location privacy plays a critical role in concealing context information, otherwise the monitored entities or subjects may be put in danger. Many traditional solutions have been proposed based on the creation of random routes, such as random walk and fake sources approach, which will lead to serious packet delay and high energy consumption. Instead of applying the routing in a blind way, this article proposes a novel solution for source location privacy in WSNs by utilizing sensor ability of perceiving the presence a mobile attacker nearby, for patient attackers in particular to increase the safety period and decrease the data delivery delay. The proposed strategy forms an intelligent silent zone (ISZ) by sacrificing only a minority of sensor nodes to entice patient attackers away from real packet routing path. The analysis and simulation results show that the proposed scheme, besides providing source location privacy energy efficiently, can significantly reduce real event reporting latency compared with the existing approaches.

Key words: source location privacy; wireless sensor networks; energy-efficiency; context-aware

CLC number: TP393 **Document code**: A **Article ID**: 1005-1120(2018)01-0203-16

0 Introduction

The sensors, due to their small size, and strong networking performance, are easy to maintain and deploy[1,2]. Sensor networks are widely used in some sensitive environments such as the battlefield, and some wild animal reserve areas. For instance, in a wireless sensor network (WSN) for monitoring wild endangered animals, an electric sensor carried by a panda can send its own information to the sensors nearby, and then the event is transmitted through the WSN to the monitor center (sink). The first sensor that receives the signals from the monitoring asset such as the panda, is called the source node, as shown in Fig. 1. An attacker in the vicinity of V_1, carrying a piece of signal detection equipment to eavesdrop, moves to V_2 according to the context information of the network such as the packet's sending time and the location of the sending node, and he will repeat this process until he approaches the source node, namely the location of the panda. In

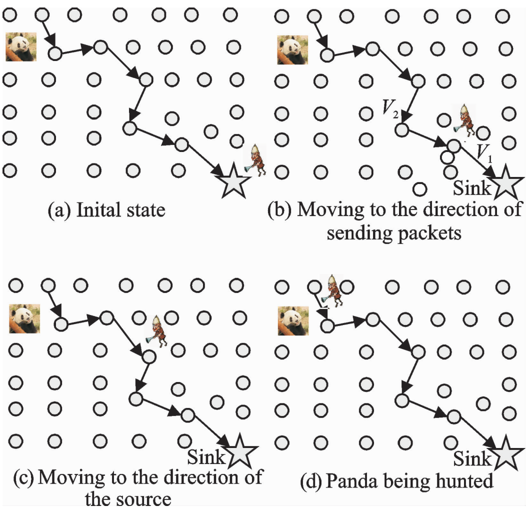

V_2
V_1
Sink
Sink
Sink
(a) Inital state
(b) Moving to the direction of sending packets
(c) Moving to the direction of the source
(d) Panda being hunted

Fig. 1 Attack based on context

* Corresponding author, E-mail address: qinxcs@nuaa.edu.cn.

How to cite this article: Zhou Qian, Qin Xiaolin, Ding Youwei, et al. Intelligent silent zone for source-location privacy based on context-awareness in WSNs[J]. Trans. Nanjing Univ. Aero. Astro., 2018,35(1):203-218.
http://dx.doi.org/10.16356/j.1005-1120.2018.01.203

the end, the privacy of the source location is disclosed.

In practice, the object sensed by the source node normally demands for key protection, so the source location should not be revealed in the process of data transmission, in order to avoid severe loss of economy or resources. As a kind of privacy information, the source location can only be visited by the authorized person. The privacy can be classified into the content-based and the context-based[3]. The content-based privacy refers to the integrity and confidentiality of the content, that is, the content cannot be tampered. The privacy discussed in this paper is based on the context, which can be obtained by attackers to infer the source location.

The prior technologies for preserving the source privacy are implemented mainly by changing or increasing the current routing paths, such as phantom routing, multi-path routing, dummy sources injection and other security routing mechanisms. These technologies may achieve a certain safety at high expense of delay or energy cost, so they are not feasible for the wireless sensor networks(WSNs) application which have high requirements of efficient energy or real-time response. For instance, the main idea of multipath[4] is that packets are sent firstly to the pseudo source, and then to the sink by single path routing or flooding. Because the attacker is not visible in WSNs, in order to choose the pseudo node[5], we need to know the entire network topology. Hence, the methods for choosing pseudo sources are normally very complex, leading to great energy cost and packet delay[6]. Furthermore, the routing with topology information is vulnerable to traffic analysis of global attackers[7].

In an event-driven WSN, the routing is normally on-demand. For a specific event, it will choose the corresponding routing strategy. For example, in a wildlife reserve, for the requirement of privacy, a security routing is applied to transmit animal information through the monitoring WSN. In addition, the sensors will work as soon as an emergency is detected, when a shortest-path routing or flooding is usually applied due to the shortest delay. However, these schemes are vulnerable for revealing the location privacy[4] easily. In order to deal with these problems, it is urgent to find a kind of secure mechanism that not only has little impact on the original routing, but also can resist the attacker′s traffic analysis[8].

With the development of hardware technologies and reduction of the cost, some monitoring sensors which are applied in critical applications, such as border surveillance and endangered animal reservation, are equipped with the sensor modules for detection of moving objects[9] and electric signals. These sensors can automatically recognize one moving attacker[10,11], and then broadcast the location of the attacker to its neighbors by beacon signals. Rios et al. proposed a greedy routing algorithm of context-aware location privacy (CALP)[12] and silent zone(SZ) scheme based on such attacker-recognition technology. However, according to the Kerckhoffs′ principle, the attacker will know the whole design of the secure system. We assume that the attacker knows the routing protocol and can decrypt the security protocol. Although CALP is also based on the shortest path, the packet would have great delay, because the privacy preserving function depends on the beacon scheduling to update the routing table every time, when the period of beacon increases. The application of beacons has brought new challenges to the network performance[13]. Despite the high privacy of SZ by isolating attackers from the whole network, the packet fails to be delivered successfully when a patient attacker stays near the sink.

The scheme presented in this study is independent from beacon frequency and can subtly entice adversaries far away from the real routing path. Therefore, as our scheme causes the least impact on the original routing, the packet can be delivered efficiently to the sink with no more delay. In this process, the location privacy is also preserved by stopping attackers from receiving any information. The main contributions of this paper are summarized as follows:

(1) We propose an intelligent silent zone (ISZ) mechanism to preserve the source location privacy, by enticing the attackers away from real packet routing path in a silent zone.

(2) ISZ can preserve the source location privacy even when the attacker knows the routing protocol. Besides, this scheme is applied in a universal scenario regardless of the routing policy.

(3) The path bias is introduced to measure the impact of secure policies on the current routing. ISZ mechanism can maintain the original path to the great extent.

1 Related Work

The research on the source location privacy (SLP) [2,14] in WSNs has been drawing significant attention. According to their abilities, attackers come in two varieties, local and global. The global[7,15] one can know the whole network traffic. In order to resist the attacker's global traffic analysis, dummy packets are usually injected in the real packet transmission interval, resulting in considerable energy cost. And the multi-path routing[6] can enhance the load balance and quality of service (QOS), which makes the global attacker difficult to track the packets[5]. The local attacker[16] can receive the information in the vicinity of him, while multiple local attackers can cooperate with one each other to get a wider range of network information[17]. As a local attacker, whose location is still invisible like a ghost to the entire network, he can analyze the network traffic to infer the source location. Previous studies have shown that there are mainly three techniques to hide the traffic. One is the phantom routing[4] proposed by kamat et al. in their panda-hunter model for the first time, which includes the first step of having random walk to a phantom source, followed by the shortest path or flooding to the sink in the end. However, as random walk increases, the packet gradually approaches the source node[4,18], indicating the revelation of the source location in turn for a random walk phase. Shortly afterwards, some improved algorithms such as greedy random walk (GROW)[19] are proposed, which are associated with more energy cost to reduce the transmission delay and improve the security. The other two schemes are dummy packets mechanism[3,20] and pseudo source node mechanism[7,21]. These two methods can resist more powerful attackers, but because the number and the location of pseudo nodes are randomly distributed, some unnecessary energy cost is unavoidable.

With the development of the hardware, the attacker will be in visible for the wireless sensor network. By using the characteristics of attacker perceiving[12], nodes relatively far from the attacker are chosen as the shortest path to the sink, which brings a new idea for solving this kind of problem. Moving object recognition technology[9-11] in resisting the attacker, enhances the certainty of the strategy, instead of randomness. However, the authorized moving objects can be allowed to enter the WSN, such as scientists detecting data in the field. Merely a simple authentication mechanism[22,23] can exclude the unauthorized migration of mobile objects. Between the external moving objects and sensors, the establishment of session key based on elliptic curve cryptography (ECC) is more simplified with smaller public key, compared with non-ECC mechanisms.

To further reduce the overhead of data transmission, according to the characteristics of the IEEE 802. 15. 4 MAC layer, Shao et al.[24] made use of the payload of beacons to transmit data, which will be extracted through programs in the application layer. In addition, the Mac layer for maintaining a reliable communication link, can also be used to broadcast information by beacons. The MAC mentioned here is beacon-enabled, and the influence of varied MAC protocols on the network performance is different. According to Ref. [25], a short interval between beacons will cause too much synchronization overhead, while a long interval will result in a longer guardian time for the time drift. The beacon interval can be adjusted adaptively according to the network traffic, such as changing the duty ratio to increase the throughput for tunable media access control (T-MAC) and sync-MAC(S-MAC)[26]. The frequency can also be changed by the software depending on the specific application. There are two advantages of using beacons to transmit the data, the first is energy saving, and the second is to hide the path.

2 Problem Description

2.1 Network model

In a homogeneous wireless sensor network, there are N nodes $\{n_i | 1 \leqslant i \leqslant N\}$, and each sensor has the same computing and storage capacity, with every node of n_i known their location(x_i, y_i) and the sink(x_s, y_s).

Assuming that the sensors are deployed in a free plane space, the distance between sensors is the Euclidean distance. If the location of node v_1 and v_2 are located respectively in (x_1, y_1) and (x_2, y_2), the distance between v_1 and v_2 is

$$d(v_1, v_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (1)$$

If there are a few neighbors in a sparse network, an attacker is easier to locate the sender near him. So the nodes of network are densely connected.

In the view of the external attacker, the format and the size of each packet is the same, and the node′ s identity information is encrypted to prevent an attacker from decrypting the contents of packets, therefore he cannot distinguish between true packets and pseudo ones.

As mentioned earilier, the attacker-recognition module can tell the location of the attacker $H(x_h, y_h)$. The authorization mechanism is introduced to eliminate the interference in the process of identifying moving objects, and the unauthorized target (with electromagnetic signal) is regarded as an attacker. The moving object authorization is ignored, for example, the scientists carry a personal device to examine the data collected in the field, so such moving object is not an attacker.

2.2 Attack model

Due to the limited communication range of each sensor node in WSNs, the packets are transmitted hop by hop. The attacker locates the base station or the data source by using the time dependence of the packets and the traffic patterns. According to the attacker′s reaction when he receives a packet, attackers come into two types[27]: (1) The patient attacker, he will not move until he receives a new packet , and then moves to the direct direction of the packet sending; (2) The cautious attacker, if he has been waiting at a node for a new packet for a fixed time, he will return back to the last location. No standards can be used to distinguish the ability of these two type attackers, for the perceptive attacker has the path analysis ability. While in some cases, the patient attacker can provide much more safety, which will be elaborated in Section 4. Therefore, when designing privacy schemes, we should take these two types of attackers into account.

We assume that the attacker is local and passive. Local means that the attacker′ s observing scope is only the sensors in his vicinity, and passive indicates that the attacker does not have any functional impact on the sensor network. The attacker knows the location of the sink node. As an external attacker, he can only eavesdrop on the packets in WSNs, but not control any internal sensor nodes.

According to the angle and the strength of the received transmission signal, the attacker strarts from the sink node and follows the direction of the direct sender to capture him. If the attacker does not receive any packets within a certain period of time T, he will have random walk to find a node sending a packet, and continue to eavesdrop. Here:

(1) If the time of T is short, it is a curious attacker;

(2) If T is infinite, it is a patient attacker.

An attacker moves at a constant speed of V_A, where $V_A \leqslant V_m$ and V_m represents the speed of packets between nodes. The eavesdropping range of an attacker is not greater than the communication range of a node, that is, $D \leqslant R$, where D and

R represent the eavesdropping range and the communication radius of the sensor node, respectively.

3 Method

3.1 Attack-preserving technology

Traditional intrusion detection system is unable to detect the attacker since the passive attacker has no affection on the whole network. While because of the inherent character of the attacker as a moving object with electromagnetic signal, sensor nodes equipped with special models can monitor and track unauthorized moving objects[28].

The sensor node applied here includes two functional models: M-DS and control mode, as shown in Fig. 2.

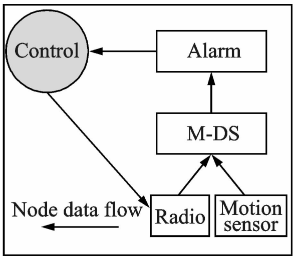


Fig. 2 Functional models

The module is used to detect whether an attacker is nearby, relying on the existing technology. If an attacker approaches, an alarm is sent by the M-DS module to the control module. The control module then transmits beacon signals to inform sensors nearby.

3.2 Silent zone scheme

SZ scheme is introduced by Rios in Ref. [12]. The main idea is that as soon as the mobile attacker is detected by the sensor nearby, the senor will notify all other neighbours of the attacker′s location, and the neighbours that receive the warning message will be set silent. All silent nodes fail to forward packets any more, even if they receive these packets and then discard them. We call these nodes as SILENT, which can be achieved by the software.

Definition 1 There are four possible states defined by an enum. SLEEP and ACTIVE are steady states and SEND is transient, and SILENT is also a transient state that the nodes will simply discard or store the packets they receive, without forwarding it.

```
enum{
INIT = 0,
SLEEP = FSM_Steady.(1),
ACTIVE = FSM_Steady.(2),
SEND = FSM_Transient.(1),
Silent = FSM_Transient.(2),
}
```

Once an attacker appears, all nodes within the security boundary are notified by the aforementioned beacons. If the node H_node is the first one that detects the attacker, it can determine the location of the attacker, and then send a beacon. Taking H_node as the center of a disk, all the sensors within communication radius R will receive the R signal and set their states to be silent.

Each node knows the location of the sink and its own, and can send information by beacon signals. Intuitively, the SZ mechanism significantly decreases the number of real packets captured by an attacker. According to the attack model in Section 2.2, the attacker will walk randomly until he captures a packet in the network. When the attacker is close to the real data transmission path, the next delivery will deviate from the original route. Such deviation will lead to an increase in the path length and the energy consumption of the network. With the increasing number of walk steps, the walk area is increasing accordingly. If the source node is close to the sink node, the attacker can find the source node in a short time by completely random walking.

In order to prevent attackers from receiving new packets by SZ mechanism, there are two disadvantages when an attacker is near the sink node: (1) It would make packets not arrive at the destination, resulting in a very low delivery rate. The corresponding solution is that when the attacker is in the vicinity of the sink, the minimum safety distance is set small, and when the attacker is far away, the minimum safety distance is changed back to the communication radius. (2) It would make the attacker easier to find the source node nearby, because no packer is captured by the attacker, and then he will have a random walk, as discussed before.

The advantages of completely isolating the attacker from real packets is obvious. The attacker can not receive any context information any more, meanwhile he has random walk. Given the current node position as $CN_0(x_0, y_0)$ after h step, the coordinate can be followed as

$$DN_{\mathrm{hwalk}} = CN_0 + CN_1 + CN_2 + \cdots + CN_{\mathrm{hwalk}} \tag{2}$$

$X = CN_i - CN_{i-1} (i > 0)$, where X is an independent distribution of random variables, namely $\{(1,0), (-1,0), (0,1), (0, -1)\}$.

$k \cdot h_{\mathrm{walk}}$ is distance from CN_0 to the location after h_{walk} step, where $\{k \mid 0 < k < 1\}$, the asymptotic probability of $k \cdot h_{\mathrm{walk}}$ is as follows

$$P = \frac{1}{h \cdot \pi} \int_0^{k \cdot h_{\mathrm{walk}}} \int_0^{2\pi} \mathrm{e}^{-r^2/h_{\mathrm{walk}}} r \cdot \mathrm{d}\theta \cdot \mathrm{d}r = 1 - \mathrm{e}^{-d^2/h_{\mathrm{walk}}} \tag{3}$$

When the number of h_{walk} continues to increase, the probability of going back to the original location for the attacker tends to 1. The attacker can only walk around for ensuring the location privacy of the source node. When the distance between the source node and the sink is relatively small, the source node is within this small range. As the h_{walk} increases, the source node could be found only in a limited time. However, it has been proved that when the source node is far away from the attacker, the probability of finding the sink node is very small. Therefore, one of the design goals in this paper is to let the attacker move away from the source node, which can be achieved as long as the moving direction of packets captured by the attacker is opposite to that of the source.

When the attacker is near the original routing path, the longer the minimum safety distance is, the more deviation of the routing path will be. It will lead to great energy consumption. Worst of all, it will result in the instability of the network. In order to make privacy protection mechanisms to be more widely used, it is necessary to let the attacker far from the source, and at the same time to remain the original routing path unbiased. The routing path bias is defined in the next section. The smaller routing path bias, the higher quality of network service.

3.3 The proposed mechanism

First, we need to define the routing path bias. The smaller routing path bias will has the less impact on the original routing path.

Definition 2 Given μ as the mean length of routing paths. When the security mechanism is applied and the length of the ith routing path is count_i, the routing path bias S^2 is defined as follows

$$S^2 = \sum \frac{(\mathrm{count}_i - \mu)^2}{n} \tag{4}$$

To minimize the routing path bias, we need to optimize SZ scheme. This article presents a novel solution called ISZ, whose main idea is that the routing for real packets is complemented outside the silent zone, and while the packet routes are near the silent zone, a false packet is sent to a bait node chosen intelligently, to entice the attacker away from the original routing path. The false packets can get through the silent zone, which will be described as shown in Table 1. Here, the greedy shortest path routing is chosen for the efficient purpose. The specific steps of ISZ will be described below.

Communication between sensors, we adopt acknowledgement mechanism to ensure the reliability of data transmission. As shown in Fig. 3, when the node A forwards a packet M to B, A will receive an implicit confirmation when B forwards the packet M downstream. If A does not hear B's acknowledgement in some abnormal situations, such as interruption of link or silent state of nodes, the node A will notify its neighbors of their current states, and then select the next hop node prior to retransmitting the packet. The blue shadow section indicates the zone or area

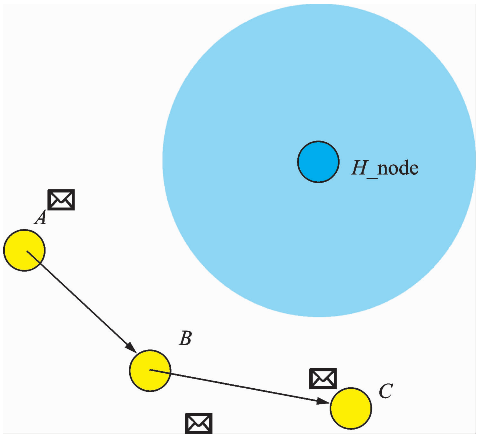
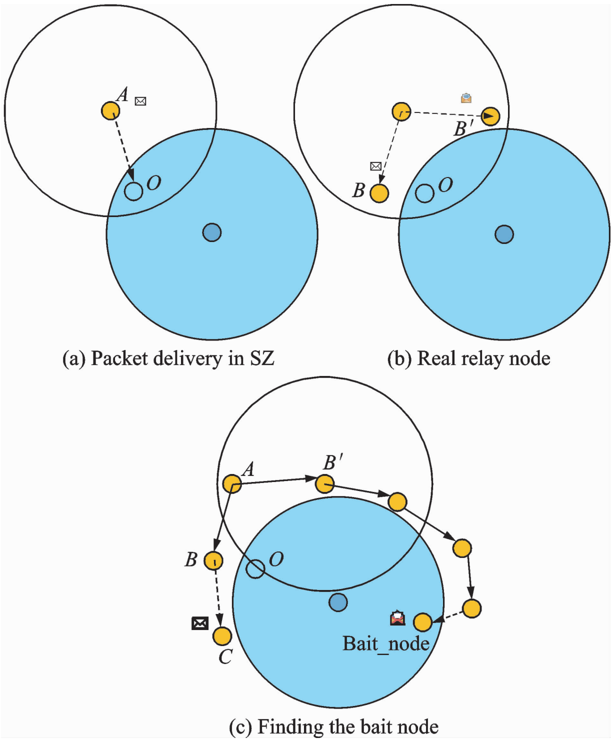


Fig. 3 Packet transmission outside the silent zone

of an attacker′s eavesdropping. Fig. 3 illustrates an attacker walking away from the delivery path of the real packet. The dashed arrow represents the state that after the node A has delivered a packet to B successfully, B is broadcasting a packet. If B receives an acknowledgement from C, the dashed arrow will change into the solid line like that from A to B.

The number of the relaying nodes and selection strategies varies depending on the routing protocols. For the greedy shortest path routing protocol, we assume that the node O is supposed to be the next hop of A. When O receives A's signal, the state of O is silent (in shadow warning area). As mentioned above, O changes into a silent state when it receives the warning beacon signal from H_node. Therefore, the packet will be discarded, as shown in Fig. 4(a). Provided that the node A cannot receive the acknowledgement from the node O, it will reselect a new relay for the real packet and simultaneously send a false packet M. The detailed process is carried out in two phases, an update phase and an operational phase.

We assume that each sensor has a list of its neighbors. In the update phase, the node A obtains all the information of its neighbor nodes which belongs to SET-Nei _ A, using one-hop broadcast message. According to the states information of neighbors, the currently active neighbors′ information is updated as SET_Active_A, where SET_Active_A=SET_Nei_ ASET_Silent_



(a) Packet delivery in SZ

(b) Real relay node

(c) Finding the bait node

Fig. 4 Illustration of a packet delivery process

Zone. In the operational phase, B and B' are chosen to be the successor of A. The node B is for the real packet M, and B′ is for the false packet $\dot{M}$, as shown in Table 1. From the perspective of an attacker, $\dot{M}$ has no difference from M. The node which receives M, will continue to deliver M to the next hop Next_Hop_Real according to the original routing outside the silent zone. While the node chosen to forward $\dot{M}$ will elect the next hop Next_Hop_Fals according to Algorithm 1.

Table 1 Two types of packets

Packet	Property 1	Property 2	Property 3
Real packet M	Deliver to the sink	Include true data	Cannot be transmitted by silent nodes
False packet $\dot{M}$	Deliver to the bait node	Include false data	Can be transmitted by silent nods

Algorithm 1 The next hop outside the silent zone

```
Input: $O$, Current_node, Nei_ Current
Output: Next_Hop_Real, Next_Hop_False
(1) SET _ Active _ Nenode ← Info _ Message (Nei_ Current);
(2) Foreach node ∈ SET_Active_Nenode;
(3) IF($d$(node, sink) < $d$(Next_Hop_Real ,
sink) )
    //deliver real packets on the greedy shortest path
    (4) Next_Hop_Real=node;
    //the node closest to node $O$;
    (5)Endforeach
    (6)Foreach node′ ∈ SET_Active_Nenode;
    (7) IF(angle(Next_Hop_Real, O, node′) > angle(Next_Hop_Real, O, Next_Hop_False))
      //The principle for choosing the false packet relay
    (8) Next_Hop_False=node′;
    //the node which is the closest to Silent Zone,
    but the further from $O$;
    (9)Endforeach
    (10)RETURN Next_Hop_False;
```

In the update phase, the node A can identify the silent nodes by the feedback from its neighbors. For example, the nodes which are geographically adjacent in the silent zone, such as O and O_1, are concluded to be in silent states because they are unable to send acknowledgements to A. The nodes which send acknowledgements are intuitively evaluated to be active, as shown in Fig. 5. Although there are some nodes that do not send signals because of other abnormal factors, such as energy depletion, one of the reasons that these nodes are not identified to be silent is that their geographical locations are not contiguous. However, such abnormal situation is beyond our scope of discussion, and there are only two states are taken into account, silent and active. After the update, as shown in Fig. 4(b), the active node B, which is closest to the sink, is chosen according to the greedy shortest path routing protocol. As each node knows the location of its own and the sink according to the neighbor list as shown in Table 2, where D denotes the distance, we also can select the node B' to forward the false packet, and the selection principle is that the node should be close to the silent zone but away from the node O. As shown in Fig. 5, $B3$ is the best node because it is further away from O than $B1$ and $B2$ and closer to the silent zone than $B4$. Obviously, B' is the locally optimal relaying node, if $\forall X, B' \in \text{SET\_Active\_}A \wedge X \neq B'$, $\angle BOX \leqslant \angle BOB'$.

$$\text{angle}(B,O,B') = \angle BOB' = \arccos\left\{\frac{[d^2(O,B) + d^2(O,B') - d^2(B,B')]}{2d(O,B)\cdot d(O,B')}\right\} \tag{5}$$

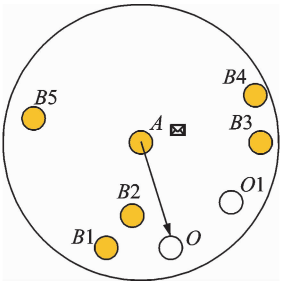


Fig. 5 Neighbours′ state

Table 2 List of A′s neighbors

Neighbors (A)	D to sink	Silent	D to A	D to $B1$	D to $B2$	D to $B3$	D to $B4$	D to $B5$
$O(x_O, y_O)$	$d(O,sink)$	1	$d(O,A)$	$d(O,B1)$	$d(O,yB2)$	$d(O,B3)$	$d(O,B4)$	$d(O,B5)$
$B1(x_{B1}, y_{B1})$	$d(B1,sink)$	0	$d(B1,A)$	0	$d(B1,B2)$	$d(B1,B3)$	$d(B1,B4)$	$d(B1,B5)$
$B2(x_{B2}, y_{B2})$	$d(B2,sink)$	0	$d(B2,A)$	$d(B2,B1)$	0	$d(B2,B3)$	$d(B2,B4)$	$d(B2,B5)$
$B3(x_{B3}, y_{B3})$	$d(B3,sink)$	0	$d(B3,A)$	$d(B3,B1)$	$d(B3,B2)$	0	$d(B3,B4)$	$d(B3,B5)$
$B4(x_{B4}, y_{B4})$	$d(B4,sink)$	0	$d(B4,A)$	$d(B4,B1)$	$d(B4,B2)$	$d(B4,B3)$	0	$d(B4,B5)$
$B5(x_{B5}, y_{B5})$	$d(B5,sink)$	0	$d(B5,A)$	$d(B5,B1)$	$d(B5,B2)$	$d(B5,B3)$	$d(B5,B4)$	0

Algorithm 2 Choosing a bait node intelligently in silent zone

```
Input: $O$, Current_node, Real_node, Nei_Current
Output: Next_Hop_False, bait_node
(1) SET_Active_Nenode ← Info_Message(Nei_Current);
(2) SET_Silent_Current = SET_Nei_Current − SET_Active_Nenode;
(3) Initialization: bait_node = $O$;
(4) While(bait_node ∉ SET_Silent_Current ∨ d
(O,bait_node)<R)
    Next_Hop_False(Current_node);//choose the next false hop according to Algorithm 1
    Current_node=Next_Hop_False;//initialize the next node
  Endforeach
  node′=$O$; //initializing node′
  Foreach node ∈ SET_Silent_Current;
    $d$(node′, $O$) = MAX($d$(node, $O$));//if more than one node meet the requirement, choose the furthest one away from $O$
    IF($d$(node′,$O$)> $R$)
      bait_node=node′;
      RETURN bait_node;
    Else node′ ∈ SET_Active_Nenode;
  Endforeach
Endwhile
```

Step 1 First, the neighbors′ states are obtained by the current node, and two sets are classified: the set of silent neighbors SET_Silent_Current and active neighbors SET_Active_Nenode.

Step 2 If there is one of the silent neighbors of the current node in SET_Silent_Curren, and this neighbor node′ meets the requirement, namely d(node′,O)> R, where R is the attack radius, node′ is the bait_node we are looking for. Otherwise, go to step 3.

Step 3 If the node′ is not in the silent zone or d(node′,O)≤R, the current node will continue to search the next hop Next_Hop_False(Current_node), which is the nearest to the silent zone, as presented in Algorithm 1. Move to the next hop, and initialize this node into the Current_node.

Repeat the above steps until the required bait_node is met, as shown in Fig. 4(c). The false packet continues to being forwarded prior to being broadcast by the bait node. The one-hop broadcast packet entices the attacker to move away from the original routing path. The nodes which receive this fake packet simply discards it. Besides, in order to select the optimal bait_node, we need to ensure our network is deployed densely.

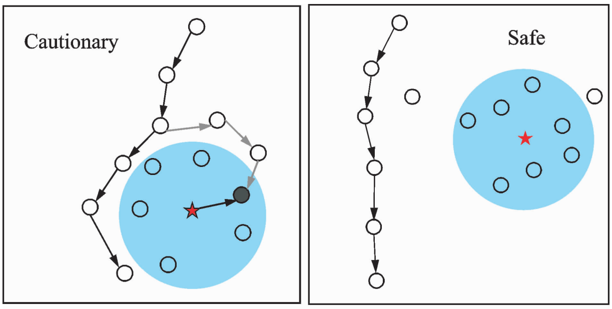
3.4 Privacy analysis

As shown in Fig. 6, the network employing ISZ mechanism will have the following two states depending on the location of an attacker. The first state is cautionary when the attacker is close to the routing path. For the contextual privacy, a longer route is chosen to avoid the attacker′s eavesdropping. In the meantime, the attacker will receive false packets from a bait_node, instead of real messages. As a consequence, the attacker will move to the bait_node, which is far away from the original routing, and achieve the second state, that is, safe state. In the safe state, the routing bias caused by the SZ mechanism will gradually disappear and the packet will be delivered by the original routing.

Definition 3 In order to measure the privacy performance of the network, for a single attacker with definite attack model, safety period and capture likelihood[4] are adopted.

(1) safety period § : The number of monitoring data sent by the source node, before the attackers capture it.

(2) likelihood L: In a fixed time , the probability that attackers capture the source node.



(a) Cautionary (b) Safe

Fig. 6 Two state models

Before the source node is captured, the more packets are sent, the longer the safety period is, and the higher the privacy level is. Within a fixed time and distance from the source node to the sink, s-d, the higher the capture likelihood is, the worse the privacy level is .

As mentioned before there are two states in Fig. 6. We assume that the probability of the network in the cautionary state is P_C. As the area of the silent zone increases to cover the attacking range, the attacker can no longer receive any real packets. Therefore, the real packet capture likelihood is 0. Meanwhile, the attacker will track the false packets. Consequently, the network changes into a safe state, whose probability is assumed to be P_S, as shown in Fig. 6(b), when the attacker can receive neither real nor false packets. For a patient attacker, he will stay there all the time (for a long time), and the privacy of the network is guaranteed, that is, the source capture likelihood is 0. For a curious attacker in the safe state, he will have random walk, so the source capture likelihood is $L = P_S / N$ (N is the number of sensor nodes in the network). When he moves close to the routing path, he will be enticed by the bait node. As a result, the source capture likelihood for a curious attacker in the cautionary state is $L = P_C \times 0 = 0$, because he will receive none of real packets and move to a false direction. So, the probability of capturing the source for a curious attacker is P_S / N, where $P_C + P_S = 1$.

As seen from Fig. 6 intuitively, the attacker does not interfere with the network in the safe state, while in the cautionary state, the length of real-packet path increases and false packets will generate extra energy. Therefore, we will briefly estimate the energy consumption theoretically, and in the next section, the performance of our proposed mechanism in the network will be verified experimentally.

3.5 Energy analysis of ISZ

Initially, an attacker starts from the sink, and the source begins to deliver the data to the sink. Assuming that the energy caused by beacons is negligible, the delay and the energy cost in the network is mainly attributed by packet transmission and reception. Therefore, the routing path length and the number of packets sent and received are mainly calculated.

In the best case, the attacker is far away from the real transmission path, as shown in Fig. 6(b). Without false packets, the energy is simply related to the routing protocol. Generally, since the shortest path costs the least energy, assuming the shortest path length is h, the total energy consumption of transmission for each event to the sink is $\overset{\frown}{E}^{\text{Safe}}_{\text{network}} = h \cdot E_{\text{sr}}$, where E_{sr} is the energy cost of the transmission and reception of each packet for a single node. The path bias is affected by the attackering area. In the worst case, the real routing path and the false path nearly circle around the attacking range, as shown in Fig. 6 (a). Let the radius of the eavesdropping area be R hops, and assuming that the real packet length is h, the total energy consumed for each event to the sink in the worst case is around $\overset{\frown}{E}^{\text{Cautionary}}_{\text{network}} \approx (h - 2 \cdot R) + 2 \cdot \pi \cdot R \cdot E_{\text{sr}}$. The average energy is $\overset{\frown}{E} = P_S \cdot \overset{\frown}{E}^{\text{Safe}}_{\text{network}} + P_C \cdot \overset{\frown}{E}^{\text{Cautionary}}_{\text{network}}$.

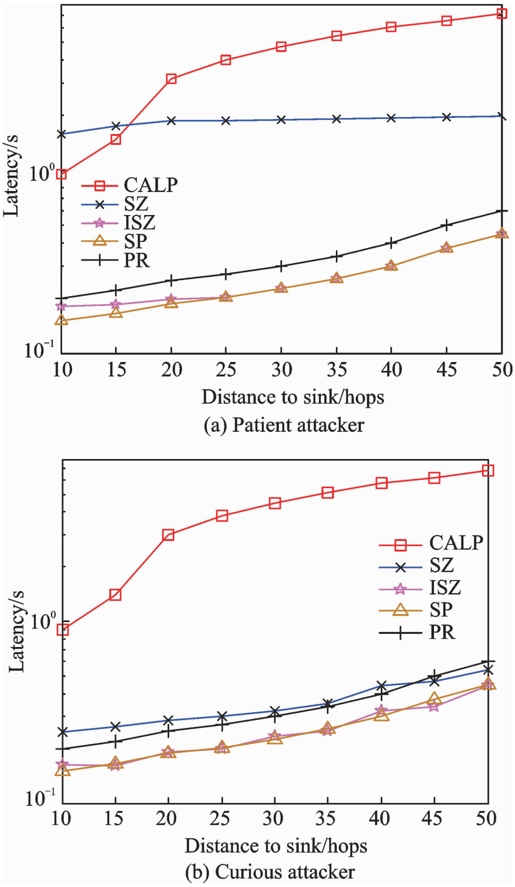
4 Performance Evaluation

A simulator Castalia based on OMnet++ is applied to verify the efficiency of our methods. We deploy a squared field of 100×100 m, where all sensors are distributed uniformly. The sink is arranged randomly in the central. Assuming that there is only an attacker, we let the monitored source asset be located in different distance from the sink. The MAC protocol is based on IEEE 802.15.4, including information load part as mentioned above. Once an attacker is detected, an alarm beacon is sent. Although ISZ does not reply on the routing protocol, in this comparative evaluation, we use ISZ based on shortest-path routing(SP), which is also applied as a baseline to reflect the impact of other approaches along with phantom routing (PR) and CALP[12]. The phantom algorithm has been discussed in the second chapter, and the process of attacker-detection in CALP is also based on the beacon technique. The main process of CALP is that each node maintains a routing table containing all its neighbors. When an attacker is found, a beacon is broadcast to update the routing table, in which the node closet to the shortest path and furthest to the attacker is chosen as the next hop node. Here we will analysis not only the curious but also the patient attacker. The beacon does not cost additional energy, but dummy packets does. The simulation is carried out for 50 times, and a total of 500 new packets are sent from the source node for each time.

(1) Delay. Delay means the sending time of a packet from the source to the sink, which includes two aspects: one is the delay caused by the beacons, and the other is packet delay due to routing policies, such as re-transmission time, routing path and etc.. Therefore, relying on the beacons to update the routing table, CALP policy have a great delay, which depends on the beacon updating frequency and the path length. The path length in CALP changes when the attack type changes. Compared with the curious attacker, the patient attacker causes much more delay in CALP, as shown in Fig. 7. Because CALP needs more time for beacons to update the routing, it causes more delay than other mechanisms.

Similar to CALP, the path bias of SZ is also affected by attack types. When a curious attacker does not receive any packets, he would be likely to walk randomly around the sink. Therefore, the delivery path to the sink is unstable, and the latency in this case is slightly higher than that in PR and SP, as shown in Fig. 6(a). Nevertheless, for a patient attacker, SZ leads to significantly higher delay than that of SP, as shown in Fig. 7 (b). Because when the attacker is near the sink, the path bias is great, leading to more than 97% of packets that can not be delivered to the sink. Suffering from great delay, some packets jump 157 hops before reaching the sink node. The delay in phantom routing is higher than that in SP for the additional steps by random walk. The phantom routing method will not be affected by the attack types, so the packet delay has nothing to do with the patient or curious attacks.

Delivery time in ISZ, similar to that in SP, only depends on the path length (i. e. , the source to the sink distance is *s-d*), regardless of beacon intervals, which have affection on network traffic. In fact, the curious attacker will have random walk for he can not receive any packets near the sink. In ISZ, it is less likely to get close to silent zones in the vicinity of source routing, so it will not cause much bias to the original path as pure SZ method does, and the increased traffic is very limited. An attacker starts from the sink and the initial data approaches to the sink when ISZ mechanism plays a role, especially for a patient attacker who will be enticed away from the original path, causing no more additional delay.



(a) Patient attacker

(b) Curious attacker

Fig. 7 Packets delay comparison using different mechanisms for two kinds of attackers

(2)Privacy. There are two main measures of privacy: safety period and capture likelihood. We conducted 50 experiments, and use the capture times to measure the source privacy in a given time. The less times to be captured are, the longer the safety period will be. The smaller the capture likelihood is, the higher the privacy will be. As shown in Fig. 8, with the increase of *s-d* , the privacy of the shortest path do not increase. On the contrary, it is the worst, because once a packet is captured, the attacker will follow the shortest path to find the source. As our experiment shown, the capture likelihood of a curious attacker is less than that of a patient attacker.

That is because the curious attacker will walk away from the sink if he waits awhile without receiving any packets. Thus, the patient attacker has a higher capture likelihood. Phantom routing in the simulation is no better than the shortest path when a patient attacker, as *s*-*d* increases, the random walk increases, the curious attacker would receive none of packets due to leaving away from the real transmission path, and lose some chances to capture sources. The essence of CALP is the greedy shortest path routing, but choosing the most furthest one from the attacker. Obviously, since CALP is related to the eavesdropping range of the attacker, in the simulation when the communication radius is set as the same as the eavesdropping range, the patient attacker can receive a few real packets in the vicinity of the sink, while the curious attacker also can catch the source after random walk if the attacker does not receive any information, when *s*-*d* is short.

Because he cannot receive any packets in SZ, the curious attacker will have random walk according to the probability distribution of random walk in Eq.(3). When the source is close to the sink, the attacker would walk to the source and capture it, as shown in Fig. 8(a). For the patient attacker, he will not receive any packets for tracing source and stay where he is. Therefore, SZ has the better privacy for a patient attacker than that for a curious attacker. In ISZ, when the distance between the sink and the source is short, the attacker has high capture likelihood for *h* is small at this time. Because of the interference by dummy packets, ISZ has more privacy than SZ when facing a curious attacker, as shown in Fig. 8(b). With the increase of *s*-*d*, the corresponding routing path *h* will increase. Both for curious and patience, ISZ has excellent performance in preserving the privacy of the source location.

(3) Path bias. According to Definition 2, the path bias shows the impact of security mechanisms on the original routing. The pure SP routing has almost no bias because the path is deterministic. Four kinds of privacy schemes are analyzed here, and the shortest path is selected as the original routing path. As shown in Fig. 9, PR has the biggest path bias, compared with other three mechanisms. The path bias of PR depends the number of hops of random walk, irrelevant to the types of attackers. The bias value for PR is unstable, because the direction of random walk is uncertain. If the direction is against the sink, the bias will increase. While if the some steps are canceled each other by random walk, the bias might just remain low.

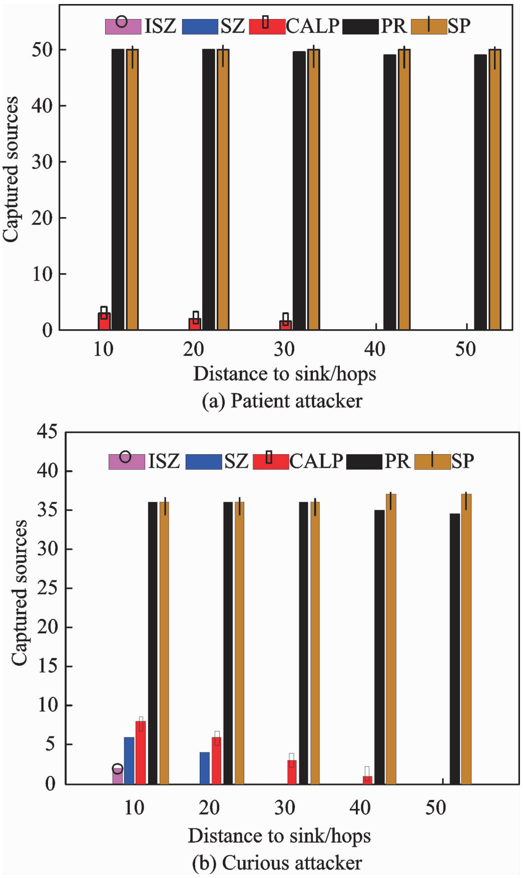


Fig. 8 Privacy performance comparison using different mechanisms for two kinds of attackers

When a curious attacker moves near the original routing path as shown in Fig. 9(b), CALP always selects the furthest node from the attacker as long as the attacker is still nearby. Consequently, the original path shifts many times. If the attacker does not receive any packets, he will have random walk, and the shift will not disappear until the attacker moves far away from the original path. In the SZ scheme, when the source is closer to the sink, that is, *s*-*d* is small, the curious attacker will capture some packets and stay on the path, resulting in a great path bias. As *s-d* increases, the curious attacker may walk randomly to a safe state, so the path bias declines relatively. The ISZ scheme causes the smallest path bias because every time when an attacker approaches near the original routing, false packets will entice him far away from the original routing, and the curious attacker will have random walk. As *s-d* increases, the probability of capturing the source becomes smaller, as well as the path bias.

When facing a patient attacker, as shown in Fig. 9(a), the bias for SZ is not found. It is because when the patient attacker is near to the sink, more than 97% of packets can not reach the sink, as mentioned before that some packets jump 157 hops before reaching the sink, leading to enormous bias. In addition, the path bias is related to the attacking range, which is set the same as the area of sensor communication. For CALP, when a patient attacker can not receive any packet, he will stay near the original path, so the bias will always exist, slightly larger than that for a curious one. The path bias of ISZ for a patient attacker is even smaller than that for a curious one. Once a patient attacker is enticed by false packets far away from the original routing, and can not receive any packets, he will no longer move. Thus the network will maintain a safe state for a long time and the following packets are delivered by the shortest path.

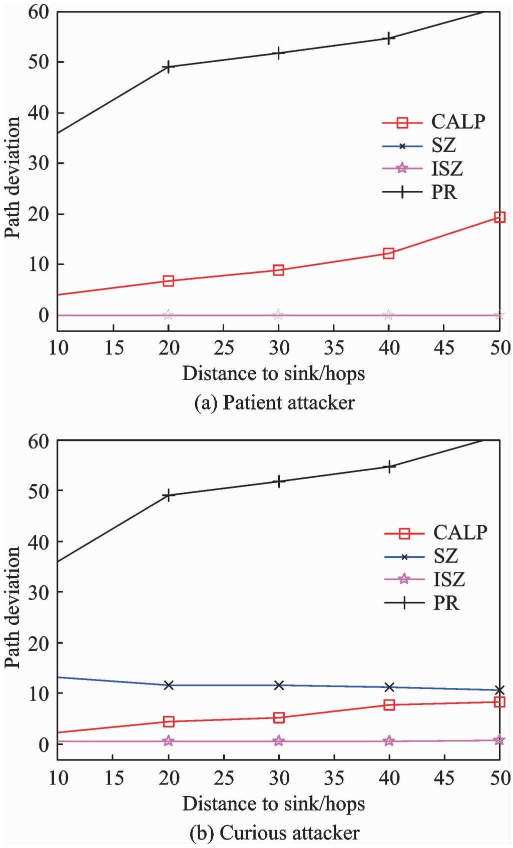
(4) Energy. The research has shown that for wireless sensors, the energy cost by executing 3 million of general program instructions is equivalent to that by transmitting data in the distance of 100 m[29].

The parameters used in this simulation are listed in Table 3.

It can be seen that with fixed number of packets and routing policies in the network, the energy consumption related to the distance between nodes is $O(d^2)$. The total amount of the energy is related to the path length squared, so the routing algorithm itself affects the energy consumption. In Fig. 10(a), the abnormal case of SZ occurs when facing a patience attacker, and the packet is always around the sink but can not arrive, which consumes much more energy. Obviously, ISZ mechanism is less likely to interfere with the original routing path. We implement the shortest path, CALP, SZ and ISZ to compare with the shortest path routing, showing the effect on the energy consumption of the whole network. Beacon scheduling itself does not generate additional energy consumption, although CALP has high delay, still maintaining the energy level of the shortest path. While for ISZ, dummy packets cause additional energy, as mentioned before, dummy packets only occur when there is a silent zone near the real routing path. In the simulation, after the attacker was tempted to leave the

Table 3 Parameters setting

Parameter	Value
$E_{\mathrm{elec}}/(\mathrm{nJ}\cdot\mathrm{bit}^{-1})$	60
$\xi_{\mathrm{amp}}/(\mathrm{pJ}\cdot\mathrm{bit}^{-1}\cdot\mathrm{m}^{-2})$	10
n	2



(a) Patient attacker

(b) Curious attacker

Fig. 9 Path bias comparison using different mechanisms for two kinds of attackers

original path, the situation is not distinct between SZ and ISZ. Therefore, when the three strategies in the face of the curious attacker, the actual difference might not be too much, as shown in Fig. 10(b). As sorted by the energy efficiency, ISZ has the best energy performance.

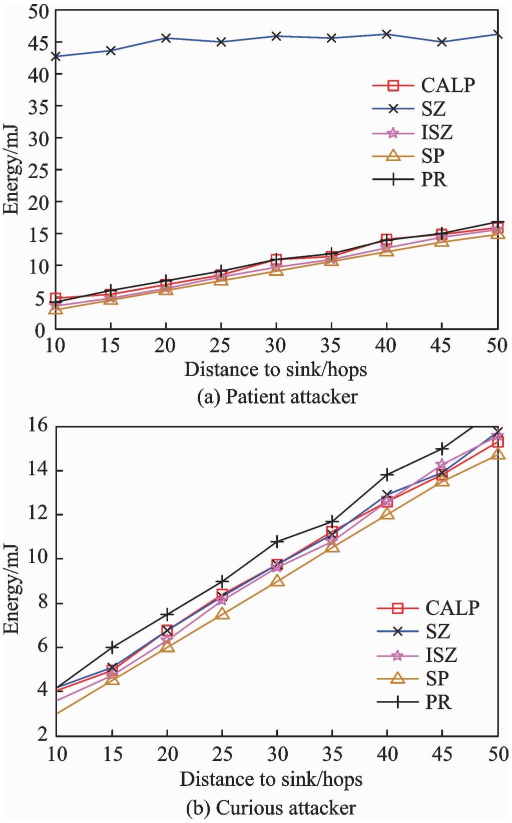


Fig. 10 Energy cost comparison using different mechanisms for two kinds of attackers

5 Conclusions

In this article, we propose an improved solution for source location privacy in WSNs, which is vulnerable to backtracking attack by a local adversary. The proposed solution of ISZ can be suitable to many event-driven WSNs applications by preventing a local attacker from receiving contextual information. Compared with SZ, ISZ combines an isolated area as a trap for adversary and entices the adversary far away from the original routing path. As shown in the results, the ISZ method outperforms its counterparts e. g. , PR and SP in the safety period as well as in energy consumption. However, cautious local adversaries as well as beaconing influence on WSNs are rarely considered. Further researches are needed to address these issues.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Nos. 61373015, 61300052, 41301047), the Priority Academic Program Development of Jiangsu Higher Education Institutions, and the Important National Science and Technology Specific Project (No. BA2013049)。

References:

[1] CONTI M, WILLEMSEN J, CRISPO B. Providing source location privacy in wireless sensor networks: A survey[J]. IEEE Communications Surveys Tutorials, 2013, 15(3):1238-1280.

[2] WANG B, ZHANG X. WSNs routing protocol of airfield lighting monitoring system based on energy balance [J]. Journal of Nanjing University of Aeronautics and Astronautics, 2015, 47(4):525-533.

[3] ZHOU Qian,QIN Xiaolin,DING Youwei. Preserving source-location privacy efficiently based on attack-perceiving in wireless sensor network[J]. Journal on Communications,2018,39(1):101-116.

[4] KAMAT P, ZHANG Y, TRAPPE W, et al. Enhancing source-location privacy in sensor network routing[C]// 25th IEEE International Conference on Distributed Computing Systems. Columbus: IEEE, 2005: 599-608.

[5] ZHANG Y, WANG G, HU Q, et al. Design and performance study of a topology-hiding multipath routing protocol for mobile ad hoc networks[C]// 35th Annual IEEE International Conference on Computer Communications. Orlando: IEEE, 2012:10-18.

[6] RAHAT A, EVERSON R, FIELDSEND J, et al. Evolutionary multi-path routing for network lifetime and robustness in wireless sensor networks[J]. Ad Hoc Networks, 2016, 52:130-145.

[7] MEHTA K, LIU D, WRIGHT M. Protecting location privacy in sensor networks against a global eavesdropper [J]. IEEE Transactions on Mobile Computing, 2012, 11(2): 320-336.

[8] YANG Y, SHAO M, ZHU S, et al. Towards statistically strong source anonymity for sensor net-

works[J]. ACM Trans Sen Netw, 2013, 9(3): 34: 1-34:23.

[9] LOURENÇO P, BATISTA P, OLIVEIRA P, et al. Simultaneous localization and mapping in sensor networks: A GES sensor-based filter with moving object tracking[C]// European Control Conference. Linz: IEEE, 2015: 2354-2359.

[10] NANDHINI S, RADHA S. Compressed sensing based object detection and tracking system using measurement selection process for wireless visual sensor networks[C]//International Conference on Wireless Communications, Signal Processing and Networking. Chennai: IEEE, 2016:1117-1122.

[11] APICHARTTRISORN D, APICHARTTRISORN K, KASETKASEM T. A moving object tracking algorithm using support vector machines in binary sensor networks[C]//13th International Symposium on Communications and Information Technologies. Surat Thani: IEEE, 2013:529-534.

[12] RIOS R, LOPEZ J. Exploiting context-awareness to enhance source-location privacy in wireless sensor networks[J]. The Computer Journal, 2011,54(10): 1603-1615.

[13] BURATTI C. Performance analysis of IEEE 802. 15. 4 beacon-enabled mode[J]. IEEE Transactions on Vehicular Technology, 2010, 59(4):2031-2045 .

[14] BRADBURY M, LEEKE M, JHUMKA A. A dynamic fake source algorithm for source location privacy in wireless sensor networks[C]// IEEE Trustcom/BigDataSE/ISPA. Helsinki: IEEE, 2015: 531-538.

[15] OUYANG Y, LE Z, LIU D, et al. Source location privacy against laptop-class attacks in sensor networks[C]// Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. New York: IEEE, 2008:1-10.

[16] RAJ M, LI N, LIU D, et al. Using data mules to preserve source location privacy in wireless sensor networks[J]. Pervasive and Mobile Computing, 2014, 11(2): 244-260.

[17] JHUMKA A, LEEKE M, SHRESTHA S. On the use of fake sources for source location privacy: Trade-offs between energy and privacy[J]. The Computer Journal, 2011, 54(6): 860-874.

[18] SHI R, GOSWAMI M, GAO J, et al. Is random walk truly memoryless: Traffic analysis and source location privacy under random walks[C]// The 32nd IEEE International Conference on Computer Communications. Turin: IEEE, 2013:3021-3029.

[19] XI Y, SCHWIEBERT L, SHI W. Preserving source location privacy in monitoring-based wireless sensor networks[C]//The 20th IEEE International Parallel Distributed Processing Symposium. Rhodes Island: IEEE, 2006:355-355.

[20] ALOMAIR B, CLARK A, CUELLAR J, et al. Toward a statistical framework for source anonymity in sensor networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(2):248-260.

[21] MEHTA K, LIU D, WRIGHT M. Location privacy in sensor networks against a global eavesdropper [C]// International Conference on Network Protocols. Beijing: IEEE, 2007: 314-323.

[22] AMIN R, BISWAS G P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks[J]. Ad Hoc Networks, 2016, 36(1):58-80.

[23] SRINIVAS J, MUKHOPADHYAY S, MISHRA D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks[J]. Ad Hoc Networks, 2017, 54:147-169.

[24] SHAO M, HU W, ZHU S, et al. Cross-layer enhanced source location privacy in sensor networks [C]//6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. Rome: IEEE, 2009:1-9.

[25] XING Y, CHEN Y, YI W. Optimal beacon interval for TDMA-based MAC in wireless sensor networks [C]// 11th International Conference on Innovations in Information Technology. Dubai: IEEE, 2015:156-161.

[26] LIU C J, HUANG P, XIAO L. TAS-MAC: A traffic-adaptive synchronous MAC protocol for wireless sensor networks[J]. ACM Trans Sen Netw, 2016, 12(1):1-30.

[27] ZHOU L, WAN C, HUANG J, et al. The location privacy of wireless sensor networks: Attacks and countermeasures[J]. Wireless Networks, 2014, 8 (5): 521- 534.

[28] BAO Y, JI C, CHEN G, et al. WSN node applied to large-scale unattended monitoring[J]. Transactions of Nanjing University of Aeronautics and Astronautics, 2016, 33(3): 386-395.

[29] POTTIE G, KAISER W. Wireless integrated network sensors[J]. Communications of ACM, 2000, 43(5): 51-58.

Ms. **Zhou Qian** received her M. S. degree in Computer Science and Technology from National University of Defense Technology in 2007. Her research interest focuses on network security, wireless sensor networks and privacy preservation. She is currently a doctoral candidate in Nanjing University of Aeronautics and Astronautics (NUAA).

Prof. **Qin Xiaolin** is currently a professor at the college of Computer Science and Technology in NUAA. His research interest focuses on security database, temporal-spatial database, data management and security in distributed environment.

Mr. **Ding Youwei** received his B. S. degree in Computer Science and Technology and M. S. degree in Computer Applied Technology both from Yangzhou University, in 2007 and 2010, respectively. His research interest focuses on energy efficient data management, cloud computing and data mining. He is currently a doctoral candidate in Computer Science and Technology of NUAA.

(Production Editor: Wang Jing)