Pers Ubiquit Comput (2016) 20:771–783
DOI 10.1007/s00779-016-0949-1

ORIGINAL ARTICLE

# An energy-efficient source-anonymity protocol in surveillance systems

**Xiaoguang Niu[1,2] · Yihao Zhang[2] · Yalan Yao[2] · Xu Chen[1] · Josep Miquel Jornet[1,3] · Jin Liu[1]**

Received: 31 January 2016 / Accepted: 12 June 2016 / Published online: 20 August 2016


**Abstract** Source-location privacy is a critical security property in event-surveillance systems. However, due to the characteristics of surveillance systems, e.g., resource constraints, diverse privacy requirements and large-scale network, the existing anonymity mechanisms cannot effectively deal with the problem of source-location privacy protection. There is an imbalance on network load and transmission latency for most of the existing anonymity schemes, which causes "funnel effect" and conflicts with anonymity. This paper proposes the dynamic optimal mix-ring-based source-location anonymity protocol, DORing. In this scheme, we first set the dynamic optimal mix-ring to collect and mix the network traffic, which can satisfy the diverse QoS requirements for all the packets. Secondly, we propose the sector-based anonymity assess to control the process of mixing in order to filter out the dummy packets and deliver the authentic packets to sink. Finally, the location of mix-ring is adjusted to balance network energy consumption, prolong the lifetime of the network and resist global attack. The simulation results demonstrate that DORing is very efficient in balancing energy consumption and transmission latency and can significantly prolong survival period of the network and ensure security as well as latency to satisfy the packets' requirements.

**Keywords** Source-location anonymity · Dynamic mix-ring · Global attacker · Degree of anonymity · Surveillance system

✉ Xiaoguang Niu
xgniu@whu.edu.cn

✉ Xu Chen
xuchen@whu.edu.cn

Yihao Zhang
yihaozhang@whu.edu.cn

Yalan Yao
ylyao@whu.edu.cn

Josep Miquel Jornet
jmjornet@buffalo.edu

Jin Liu
jinliu@whu.edu.cn

[1] State Key Laboratory of Software Engineering, Wuhan University, Wuhan, China

[2] School of Computer Science, Wuhan University, Wuhan, China

[3] University at Buffalo, The State University of New York, Buffalo, NY, USA

## 1 Introduction

Wireless-sensor-network-based event-surveillance systems are vulnerable to various security threats due to the wireless communication mode and its own limited resources. For such surveillance systems deployed to monitor real events, event source-location privacy is becoming one of the major obstacles that restrict the smart application deployment [1]. These surveillance systems face several serious challenges that include uncontrollable environment, resource constraints on the nodes and the restricted topological structure [2–4]. In the meantime, they are often in a harsh environment without maintenance in practical applications, which leads to some potential malicious attacks [5]. The event source-location privacy must be guaranteed because of its high sensitivity as well as significance [6]. For instance, it is capable of tracking military targets if sensor nodes are deployed in a battlefield [2, 7, 8]. Owing to its unique characteristics, conventional

anonymity technology is not applicable in such systems [9]. An attacker has the ability to eavesdrop the wireless communication in sensor networks. Furthermore, it is possible for him to locate the source node through traffic analysis and tracing back hop by hop without destroying the nodes, cracking the content of data packet or disrupting the proper functioning of the network. Therefore, it is a challenge to provide the source-location privacy in event-surveillance systems.

To solve this problem, a number of source-location anonymity schemes have been proposed, which are mainly divided into two categories [10]: transmission perturbation-based source-location anonymity protocol in the phase of data packet transmission and source generalization-based source-location anonymity protocol in the phase of packet generation. For the former, it mostly defenses against attack of location privacy in the model based on hop-by-hop tracing and local monitoring. However, it does not work in the face of the attack based on traffic analysis with global monitoring. For the latter, it can effectively resist almost all of source-location privacy attacks to mislead the attacker, whereas abundant fake data injection causes high network load, high network latency, poor transmission quality and many other defects. How to achieve a balance between efficiency and energy consumption is one of the key issues.

Due to the resource limitation in such surveillance systems, it is necessary to compromise security and resource utilization when we design its security protocol to achieve the highest performance with the lowest cost.

Aiming at the characteristics of event-surveillance systems and the source-location anonymity threats they faced, this paper proposes DORing, the dynamic optimal mix-ring-based source-location anonymity protocol: Firstly, in order to resist traffic analysis which are initiated by sophisticated global adversaries, all nodes in the networks inject data packets into the networks according to a certain strategy at the same time interval distribution regardless of whether event has been monitored. Secondly, energy-consumption-optimal-based mix-ring has been established in the network dynamically, which acts to separate the packets after disrupting its correlation, and make deep cuts in traffic near the base station on condition that preventing adversaries from locating packet source node via reverse back. In order to quantify the effect of source-location privacy protection after mixing the packets, we have designed a mechanism to measure the anonymity.

In summary, this paper makes the following contributions:

1. According to the non-equilibrium distribution characteristic of event-surveillance systems in energy consumption and transmission latency, the dynamic optimal mix-ring-based source-location anonymity protocol, namely DORing, is proposed which can filter out dummy traffic while ensuring the anonymity of authentic data packets and evaluating the anonymity for the packet-mixing process quantificationally.
2. By adjusting the location of mix-ring dynamically, the distribution of network energy consumption is changed and the energy consumption model under different mix-rings is established. And to get the optimal adjustment strategy of mix-ring by solving the model can achieve long-term energy efficiency and prolong the survival period of network as much as possible.

The rest of the paper is organized as follows: In Sect. 2, the related works of source-location privacy in wireless-sensor-network-based event-surveillance systems are reviewed. After that, the system model and design goals are described in Sect. 3. Section 4 details the proposed DORing protocol. Simulation experiments and security analysis are provided in Sect. 5. Finally, we conclude this paper in Sect. 6.

## 2 Related work

### 2.1 Perturbation-based source-location anonymity protocol

The phantom routing source-location privacy protocols are based on the idea of random walk [11–13]. Several limitations exist in most of these schemes, such as deep delay and low reliability in message transmission and expensive overhead in routing maintenance. Aiming at these problems, mixing ring-based source-location anonymity scheme has been proposed [14, 15]: Part of nodes in network are chosen to form the mix-ring in order to collect and mix the authentic/dummy sensing data packets. Then, the packet is forwarded to the base station when the degree of confusion meets the requirement. Rios and Lopez [16] exploit the perception ability of sensor nodes for the location information of mobile adversaries in the vicinity, choosing an approximate shortest path to base station dynamically. Greedy random walk (GROW) is proposed to reduce the chance of crankback through the increase in random walk length, which expands the route scope [7]. When a sensor node randomly transmits the packet, it is necessary to select one of its neighboring nodes that have not taken part in the random walk. In order to effectively protect source-location privacy and decrease energy consumption, Lightfoot et al. studied a Sink Toroidal Region (STaR) routing protocol [17]. The protocol contains two parts. The first part is to pass the message from the source node to a random intermediate node placed in a pre-designed area that is near the sink and referred as the STaR.

In the second part, the intermediate node transmits the packet to the sink by means of shortest path routing. Although it achieves good results of privacy protection with low energy consumption and small delay in STaR, the greatest disadvantage is that the source-location privacy is easy to leak once the eavesdropper observes the STaR for enough time leading to the exposure of the area information. The directed random walk (DROW) is proposed to reduce energy as well as transmission delay with providing a certain degree of source-location privacy protection [18]. In DROW, one sensor node is able to acquire the position of all its neighboring nodes in some way. The source sensor node delivers the packet via unicasting the packet to its parent node after finding the target. Then, this packet is transmitted from the intermediate node to one of its parent nodes with equal probability. Unless one packet is directional random when it arrives at the base station, it will be transmitted all the time. However, these perturbation-based source-location anonymity technologies cannot resist the global adversaries, which can get the source location via eavesdropping and analyzing the traffic of the entire network.

### 2.2 Source generalization-based anonymity protocol

In order to solve the problem that perturbation-based source-location anonymity protocol cannot resist global eavesdropping and traffic analysis, Mehta et al. [19] firstly proposed period acquisition-based source-location anonymity protocol: Every node in the network transmits packets at a constant rate no matter whether event has been monitored. The advantage of this approach is that source-location privacy can be protected to the greatest extent, but it will incur the huge delay and energy consumption. In order to achieve a trade-off between security property and performance, the concept of statistical intense source anonymity has been presented [20, 21], in which the packet transmission characteristic of all nodes in the network is of the same statistical significance and the source location cannot be identified, even if they are sophisticated global adversaries. However, the statistical characteristic-based scheme involves dummy packet injection from all nodes, which not only leads to a lot of energy cost but also increases the probability of packet collision as well as decreases the transmission efficiency. Zhang et al. [22] presented an all proxy scheme (APS) via injecting fake message for purpose of resisting global attacks, thus preserving the source-location privacy. In this scheme, fake message will be filtered whatever sensor nodes so as to lessen network load and achieve the high packet forwarding rate. Influenced by the fake source technique, Arshad et al. designed an algorithm using two parameters, which include message rates and fake message transmission duration to solve the problem of the source-location privacy protection [23]. In the scenario, once the source node observes the target object, one of several nodes will be picked up as the fake node to replace the real source. Furthermore, the fake node can continuously forward packets in the network, which makes the attacker mistake the fake for the real. Experiments show that adjusting two parameters properly can get different levels of privacy protection even the optimal solution while the real source location is secure. The defect of the algorithm consists in the fact that it has got to work for a grid structure network. Ortolani et al. designed the unobservable handoff trajectory (UHT) protocol through rendering event unobservable in order to deter eavesdroppers from obtaining the source-location information [24]. The injection of dummy message during the packet transmission makes it tough for the eavesdropper to distinguish the real event from other events. Simulation results indicate that eavesdroppers are incapable of acquiring which one is true even though they get the dynamic of all the events, thus hiding the event's real trajectories. In the meantime, the supererogatory communication delay does not exist among these nodes. Real events will select the optimal route to the base station so as to diminish the network overhead. The additional scheme of dummy packet injection has been improved [12, 25–29]: selecting nodes with geographic diversity as the dummy source nodes or as the agents in charge of converging packets in adjacent area to filtrate and dummy packets. In general, the source generalization-based source-location anonymity schemes can effectively resist all source privacy attacks. However, the additional injection of dummy packets will incur network load, decrease transmission reliability and aggravate the contradiction between network lifetime and event reporting delay.

## 3 System model and design goals

### 3.1 Network model

As shown in Fig. 1, nodes in the event-surveillance system are centered at the base station and distributed evenly. Let $N$-hop denotes the network radius, $R$ is the radius of communication between a node and its neighbors and $\theta$ is the density of nodes. Then, the number of nodes in the network is:

$$N_{All} = \pi N R^2 \cdot \theta \tag{1}$$

Each node can only communicate directly with its adjacent nodes on the same and adjacent ring. The sink is the only destination for all transmissions. Each message contains a unique number, which is associated with its source location.

The content of the message is encrypted through public key between nodes and the sink. All nodes have a thorough knowledge of relative location between each other, and every node has information of its adjacent nodes.

### 3.2 Attacker model

In this paper, we assume that the adversaries have the following characteristics:

1. The adversaries have sufficient energy and memory resource, adequate computation capability. They could reckon the last direct sending node by analyzing the intensity and orientation of the received information. We assume that the event can be captured as long as an adversary is in the vicinity;
2. The adversaries have strong ability to launch attacks, such as deploying multiple monitoring points and equipping with powerful audio monitors, so they have a global view to eavesdrop the traffic of entire network;
3. The adversaries only launch external (passive) attacks by eavesdropping and analyzing the traffic of entire network. This is because initiative attacks are easy to be monitored and adversaries are assumed to be unable to decode the secret key.

### 3.3 Design goals

The zero-sum game between privacy and performance has been an indisputable obstacle to deploy most existing source-location privacy schemes. Consequently, the imbalance between quantity of network service and resource consumption is aggravated, privacy is diminished and survival period of the network is shortened. In order to break away from this tradeoff, we propose a mechanism, which can optimize proportionality of energy consumption, balance the report delay and prolong the network lifetime under the premise of ensuring the source-location privacy.

## 4 DORing: dynamic optimal mix-ring-based source-location anonymity protocol

In this paper, we propose DORing, a dynamic optimal mix-ring-based source-location anonymity protocol. Nodes with same hop counts from base station form a "ring." One of the rings is selected via strategy to mix the data packets from entire network, which is called "mix-ring." The ring takes charge of filtering out dummy packets injected from network nodes and reducing energy consumption under the premise of ensuring the anonymity of packets. The architecture of DORing is shown in Fig. 2.

All nodes inject bogus traffic at a same strategy, which guarantees to send authentic packets and dummy packets to the mix-ring at the same time interval distribution no matter whether event has been monitored. Source anonymity of packet is provided in this phase; two kinds of packets are received continuously and mixed in the mix-ring to break the path relationship so that the adversaries cannot locate the source node of packets through traffic analysis. Authentic packets will be sent to the base station while ensuring its source-location anonymity and the dummy packets will be discarded. In this phase, the degree of anonymity evaluation mechanism is used to evaluate the effect of mixing and quantificationally control the process; considering the heavy workload and high energy consumption, the mix-ring should be selected dynamically in order to balance energy consumption and prolong survival period of the network.

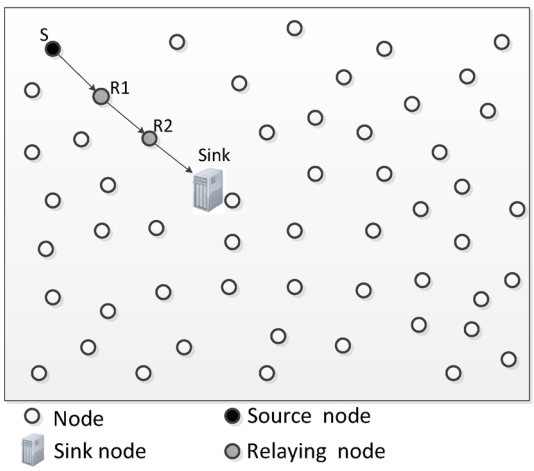



**Fig. 1** An example of event-surveillance application

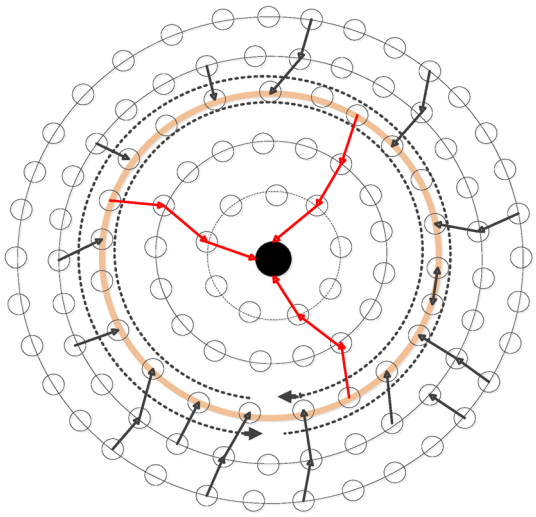


**Fig. 2** Topology of DORing-based surveillance systems

### 4.1 The network initialization and the mix-ring establishment

In the initial stage of the network, the base station will send Beacon packets that include control information, hop value *Hops* and the public key $K_{BS\_pub}$ to all the nodes in the network in a broadcasting way. The nodes can acquire their hops, make the hops $h$ in the Beacon plus one and broadcast them after receiving these packets. And the final nodes can obtain the adjacent nodes' information of their own rings and their adjacent rings. The nodes will have a key agreement with the nodes on adjacent rings and the adjacent nodes on the upper and lower rings after acquiring their location information to get the symmetric secret key $K_s$, which is used for packet transmission among subsequent nodes. After the network topology is determined, the nodes in the outermost layer of the network will send network scale *Ns* back to the base station, which means that the base station gets the entire network topology. Then, the base station broadcasts the Update packets that include the mix-ring hops RingHop and the base-station public key $K_{BS\_pub}$ to all the nodes.

### 4.2 Data transmission and piggybacking mechanism

To prevent the network from global attack, every node needs to simulate the authentic source node by injecting dummy packet periodically even if no event has been monitored. For those identical nodes, the time intervals between packets transmissions follow an identical statistical distribution such as constant rate ConsteRate and exponential distribution-based FitProbRate. For every injection scheme, the newly increased traffic in the network per unit time is:

$$F_{All} = N_{All} \cdot \frac{1}{\mu} \tag{2}$$

where $\mu$ is the mean of transmission time intervals, $N_{All}$ is the total number of nodes in the network.

When a node detects an event and gets the event data (*Data*), the public key ($K_{BS\_pub}$) shared between nodes and base station is used to encrypt the event data field: $M_{data} = \mathrm{En}(Data, K_{BS\_pub})$; then, part of the packet fields such as authentic/dummy flag, anonymity degree and event information is assigned to encapsulate the date packet: $Pkt = M_{data} \| info$; finally, the node encrypts the packet via the communication secret key ($K_{A,B}$), which is generated by negotiating with its next-hop node $B$: $S = \mathrm{En}(Pkt, K_{A,B})$, and sends the encrypted packet to the mix-ring along the shortest path. The whole process performs encryption and decryption hop by hop.

Since numerous dummy packets generated from the whole network need to be transmitted by intermediate nodes between source node and the mix-ring, these intermediate nodes could utilize these packets to piggyback authentic event information, which not only reduces the report delay of authentic event but increases the source-location anonymity. After data packet $S$ is received by intermediate node $B$, $K_{A,B}$ will be used to decrypt the packet $Pkt = \mathrm{De}(S, K_{A,B})$. Based on the information $n$ of *Pkt*, the authentic packets could be distinguished from the dummy ones: (1) If *Pkt* is an authentic packet, node $B$ encrypts the packet via the communication secret key ($K_{B,C}$), which is generated by negotiating with its next-hop node $C$: $S_T = \mathrm{En}(Pkt, K_{B,C})$, and transmits the packet to node $C$. (2) If *Pkt* is a dummy packet and an authentic packet $Pkt_T$ is waiting on node $B$ to be transmitted, the dummy packet (*Pkt*) will be replaced with the authentic one ($Pkt_T$) before encrypting and transmitting. If no authentic packet on node $B$ needs to be transmitted, the dummy packet will be encrypted: $S_T = \mathrm{En}(Pkt, K_{B,C})$ and transmitted to next node $C$.

**Procedure 1**:Transmission and Piggybacking Mechanism of normal nodes

```
1:  Input: packet from the upstream node S
2:  Parameters set ={ the flag of receiving S S_FLAG, the flag of local
                S ready to send S_L_FLAG}
3:  if(S_FLAG==true) then
4:      decrypt, Pkt=De(S,K)
5:      if (Pkt.Flag == T AND Pkt.dst==BS) then
6:          encrypt, S_next=En(Pkt, K_next)
7:          send S_next to next node towards the base station
8:      end if
9:      if (Pkt.Flag == T AND Pkt.dst==RING) then
10:         set info
11:         encrypt , S_next=En(Pkt, K_next)
12:         send S_next to next node towards the mix-ring
13:     end if
14:     if (Pkt.Flag == F AND Pkt.dst==RING AND S_L_FLAG
            ==true) then
15:         discard Pkt, send S to next node towards the mix-ring
16:     end if
17: end if
18: if(S_L_FLAG ==true) then
19:     Calculate interval, set latency time
20:     send S to next node towards the mix-ring after the latency time
21: end if
```

This mechanism of normal nodes is shown in Procedure 1 in detail.

### 4.3 Mixing and anonymity mechanism

Once a packet is received by the first mix-ring node, the node will select a movement direction either clockwise or anticlockwise with same probability. Then, the packet is mixed in mix-ring after arriving at the ring in order to eliminate the correlation between the packet and the source node.

#### *4.3.1 The mixing process in one node*

When a packet has been received by mix-ring node, it will be inserted into a corresponding buffer queue with a random order so that the sequence of the packet entering/

leaving the node can be randomly disturbed. Since the value of information field in the packet will be changed and hop-by-hop encryption mechanism is adopted, the ciphertext of the packet changes while entering and leaving a node. The adversaries cannot infer the packet path from the correlation of ciphertext; we show this in Fig. 3.

For the buffer queue of packets in a node of mix-ring, heavy traffic will result in an increase on expectation of packets' waiting delay, and low traffic will cause a decrease on the number of packets involved in mixing so that packets need to mix between nodes through a large number of times to achieve the source anonymity. Therefore, it is necessary to control the traffic in mix-ring within a reasonable range. There are two buffer queues in each node to store the traffic from two directions; the maximal length of each queue is $L$, which represents the number of packets lingering in the queue at the same time, as shown in Fig. 4.

After a packet has been received by a node, it will be inserted into the same direction buffer queue. If the length of corresponding queue exceeds L, then discard a dummy packet which has minimal hop counts (*Hops*) in the queue.

If all packets in the queue are authentic, then the authentic packet that has biggest Hops to the base station is transmitted. Each queue transmits a packet selected randomly from the corresponding queue to the same directions in every time interval *INTVL*.

The probability of a packet being transmitted out in $k$th time is:

$$P_{fwd}(k) = \left(\frac{L-1}{L}\right)^{k-1} \cdot \left(\frac{1}{L}\right) \tag{3}$$

The times expectation of waiting to be transmitted is:

$$E(k) = \sum_{i=1}^{\infty} i \cdot \left(\frac{L-1}{L}\right)^{i-1} \cdot \left(\frac{1}{L}\right) \tag{4}$$

Different event reports have diverse latency requirements. For a packet with ambitious delay requirement, it will be selected firstly so that the packet can complete mixing and be transmitted to the sink as soon as possible.

### 4.3.2 Anonymity degree measure

The mechanism is used to measure the degree of packets' source-location privacy protection in the process of mixing.

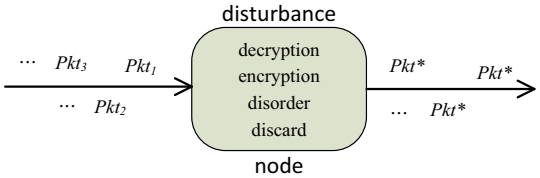



**Fig. 3** Packet disturbance in a node

As shown in Fig. 5, the network centered at the base station is divided into $Q$ sectors, which is numbered $0, 1, 2, \ldots, Q-1$.

In this protocol, bit is used to identify the sector. According to its own sector number $SecID (0 \le SecID \le Q-1)$, the node sets the source sector identification of the packet as soon as the packet is generated by source node: the $SecID$th bit is set to 1 and the rest is 0 (i.e., $SecBit = 1 \ll SecID$) to indicate the packet is from the sector $SecID$.

Some bits have been set to 1 in source sector identification $SecBit$ *to* indicate the sectors in which the source node may be located. Since the sequence of packets going through a node is completely random, the sectors which are identified in source identification are likely to be the area of the packet where it comes from. So the source identification changes as follows:

$$\begin{aligned} &SecBit_i \\ &\quad = SecBit_i | (1 \ll Src_1) | (1 \ll Src_2) | \ldots | \left(1 \ll Src_{Np}\right) \\ &\quad (i = 1, 2, \ldots, Np) \end{aligned} \tag{5}$$

After mixing, the source identification of all $N_p$ packets in the queue is the result of each packet successively

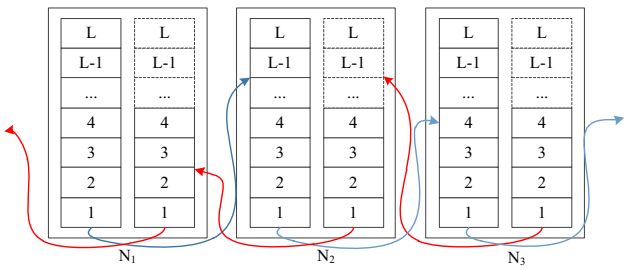



**Fig. 4** Schematic diagram of packet forwarding and mixing among nodes

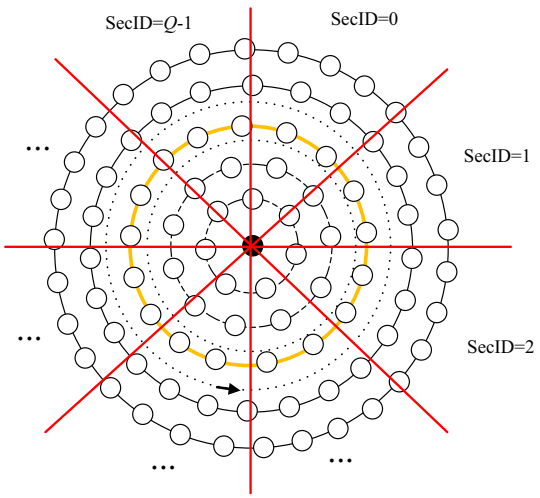



**Fig. 5** Sector division in DORing-based surveillance systems

performs a bitwise OR on its source sector number bit set 1 and their own original source identification.

#### 4.3.3 Packets elimination on mix-ring

It is necessary to eliminate the packets from the mix-ring, which have met the requirement of anonymity after adequate mixing in the mix-ring. The degree of anonymity is chosen as the standard for packets elimination.

The threshold of anonymity degree field *Anony* in packet represents the source node's requirement of the degree of anonymity for the packet, i.e., the ratio of the number of sectors which represent possible source of the packet after mixing to the total number of network sectors $Q$ can't less than *Anony*.

Since there are two directions of traffic on the mix-ring, we denote a packet as $P$ and a packet in the reverse direction queue(*Queue**) as $P$ which on the same node with $P^*$. If the ratio of bitwise OR of $P$ and $P^*$ to the section number $Q$ reaches the *Anony* of packet $P$, we consider it meets the requirement of the source node anonymity and the two packets can be eliminated:

$$\begin{aligned} &\exists P \in Queue, \quad \exists P^* \in Queue^* \\ &SecNum(P \cdot SecBit | P^* \cdot SecBit)/Q > P \cdot Anony \end{aligned} \tag{6}$$

where $SecNum(v)$ denotes bit numbers of 1 of $v$.

If the packet $P$ is a dummy packet, we discard it directly. Otherwise, forward the packet to the base station directly.

#### 4.3.4 Dynamic adjustment for mix-ring

While a large number of data packets are transmitted through the mix-ring, the energy consumption in mix-ring is much larger than other ring. It is necessary to adjust the location of mix-ring so that it can achieve the balance of each ring and prolong the lifetime of the network.

In sensor networks, the energy of nodes is mostly used for communication. In this paper, we only choose energy consumption of communication as measurable indicator. Denote the energy consumption for a node receives a packet as $\alpha$ and transmits a packet as $\beta$. The energy consumption of each node in mix-ring $Rh$-hop is:

$$Engy(Rh) = \begin{cases} \left((\alpha+\beta)\cdot\sum_{i=x+1}^{Ns} F(i) + \beta\cdot F(x)\right)/Nr(x), & x > Rh \\ \left((\alpha+\beta)\cdot\sum_{i=1}^{x-1} F(i) + \beta\cdot F(x)\right)/Nr(x), & x < Rh \\ \alpha\cdot\left(\sum_{i=Rh+1}^{Ns} F(i) + \sum_{i=1}^{Rh-1} F(i)\right)/Nr(Rh) + 2\cdot\dfrac{\alpha+\beta}{INTVL_{Rh}}, & x = Rh \end{cases}, \tag{7}$$

where $Rh = (1, 2, \ldots, N)$, $Nr(x)$ denote the number of nodes in the $x$th hop ring. The matrix of energy consumption ratio is:

$$M_{engy} = \begin{bmatrix} e_{1,1} & e_{1,2} & e_{1,3} & \cdots & e_{1,N} \\ e_{2,1} & \ddots & & & \\ e_{3,1} & & \ddots & & \\ \vdots & & & \ddots & \\ e_{N,1} & & & & e_{n,N} \end{bmatrix} \tag{8}$$

The $k$th row indicates the average energy consumption for nodes in each ring if the mix-ring on $k$th hop.

The working time for choosing the $k$th hop as the mix-ring is denoted as $Tr_k$. It is necessary to maximize $\sum_{i=1}^{Ns} Tr_i$ to prolong the network lifetime. Then, different rings should be chosen as the mix-ring on the optimal strategy, thus making full use of the energy consumption to achieve the highest energy efficiency.

The total energy of each node is denoted as $E_{max}$ to get a linear programming function whose objective function is the maximal total time of each ring becoming the mix-ring, which means the longest survival time. The total energy consumption of nodes at each ring is no more than $E_{max}$. Solve the following function to get $Tr_i(1 \le i \le Ns)$ that denotes the time ratio of each ring to be the mix-ring.

$$\begin{aligned} \max \quad & z = Tr_1 + Tr_2 + \cdots + Tr_{Ns} \\ s.t. = & \begin{cases} E_{1,1}\cdot Tr_1 + E_{2,1}\cdot Tr_2 + \cdots + E_{Ns,1}\cdot Tr_{Ns} \le E_{\max} \\ E_{1,2}\cdot Tr_1 + E_{2,2}\cdot Tr_2 + \cdots + E_{Ns,2}\cdot Tr_{Ns} \le E_{\max} \\ \vdots \\ E_{1,Ns}\cdot Tr_1 + E_{2,Ns}\cdot Tr_2 + \cdots + E_{Ns,Ns}\cdot Tr_{Ns} \le E_{\max} \\ Tr_i \ge 0 \quad (i = 1, 2, \ldots, Ns) \end{cases} \end{aligned} \tag{9}$$

The workflow of packet mixing on the mix-ring is shown in Procedure 2, and the workflow of packet generation on normal nodes is demonstrated in Procedure 3.

## 5 Performance evaluation and security analysis

### 5.1 Performance analysis

The total number of nodes in the network is:

$$N_{All} = \pi(NR)^2 \cdot \theta \tag{10}$$

The number of nodes in $x$th hop can be calculated as:

$$\begin{aligned} Nr(x) &= \pi(xR)^2 \cdot \theta - \pi((x-1)R)^2 \cdot \theta \\ &= (2x-1)\pi\theta R^2 \end{aligned} \tag{11}$$

So the number of packets received by each node per unit time on $Rh$th mix-ring is:

$$PN(Rh) = (N_{All} - Nr(Rh)) \cdot \frac{1}{\mu} \cdot \frac{1}{Nr(Rh)} \tag{12}$$

Since each node in the mix-ring can mix with a new packet from outside mix-ring, the transmission interval of the mix-ring to send packet satisfies the following constraint:

$$INTVL_{Rh} \geq \frac{1}{PN(Rh)} \tag{13}$$

Considering the equality of the time for the packets forwarding on the different mix-rings, we set $\omega$ to represent the rotational speed in the network:

$$\omega = INTVL_{Rh} \times Nr(Rh) \tag{14}$$

So above parameters satisfy the inequation constraints:

$$\begin{aligned} INTVL_{Rh} &= \frac{\omega}{Nr(Rh)} \geq \frac{1}{PN(Rh)} \\ \omega &\geq \frac{\mu}{(N^2 - 2Rh + 1)\pi\theta R^2} \quad (Rh = 1, 2, \ldots N) \end{aligned} \tag{15}$$

As for the delay of packet in the path from the source node to the mix-ring, we only take the waiting delay on the source node into consideration instead of the time when packets are processed and forwarded on the forwarding nodes. The area closer to the mix-ring can use the real data, which is piggybacked by the fake packets from upstream because of adopting the piggyback mechanism, thus leading to the fact that the delay is smaller in the area closer to the mix-ring. Set the frequency produced by the real packets is

**Procedure 2**:the workflow of packet-mixing on the mix-ring

```
Input: the packet out of the ring S_out , the packet in the ring S_in
Parameters set ={receiving S_out flag S_out_FLAG, receiving S_in flag
S_in_FLAG, the queue length L_temp, the timer trigger icon T_FLAG,
the direction of motion D, the queue head Pkt }
Set timer
if(S_out_FLAG==true) then
    decrypt, Pkt=De(S,K)
    select D randomly, insert into queue , adjust SecBit
    if(L_temp >L) then
        discard a dummy packet
    end if
  end if
if(S_in_FLAG==true) then
    decrypt, Pkt=De(S,K)
    insert into queue, adjust SecBit
    if(L_temp >L) then
        discard a dummy packet
    end if
end if
if(T_FLAG==true) then
    if(B(Pkt.SecBit|Pkt*.SecBit)/Q≥Anony AND
      B(Pkt.SecBit)/Q≥Anony/2) then
        Set Pkt.dst=BS,
        encrypt ,S_next=En(Pkt, K_next)
        send S_next to next node towards the base station
    else
        encrypt, S_next=En(Pkt, K_next)
        send S to next node towards the mix-ring
    end if
end if
```

$\lambda$/(unit area $\times$ unit time).When the mix-ring hop is $Rh$, the waiting delay on each ring is:

$$SrcDelay(Rh, x, \lambda) = \begin{cases} \dfrac{Nr(x)/\mu}{\sum_{i=x+1}^{Ns} Nr(i)/\mu - \left(\pi(Ns \cdot R)^2 - \pi((x-1)R)^2\right) \cdot \mu \cdot \lambda} \cdot \mu, & x > Rh \\ \dfrac{Nr(x)/\mu}{\sum_{i=1}^{x-1} Nr(i)/\mu - \pi(x \cdot R)^2 \cdot \mu \cdot \lambda} \cdot \mu, & x < Rh \end{cases} \tag{16}$$

### 5.2 Performance evaluation

In the simulation experiment, the radius of communication between the nodes is 30 m and the density of nodes is 1 per 330 $m^2$. The network is divided into 16 sectors. This paper compares the energy consumption, latency and other indicators of the network under different anonymity thresholds, queue lengths and network scales.

**Procedure 3**: the workflow of normal nodes

1: **Input**: Beacon packet $B_{Pkt}$ , Update packet $U_{Pkt}$
2: **Parameters** set = { detected event occurrence flag *D_FLAG*, event message *Data*, control message *info*, *Flag* $\in$*info* }
3: **Output**: *S*
4: initialize $B_{Pkt}$, negotiate with adjacent nodes
5: get *RingHop* $\in U_{Pkt}$ , $K_{BS\_pub} \in U_{Pkt}$
6: **if** (*D_FLAG*==true) **then**
7: encrypt, $M_{data}$ =En(*Data*, $K_{BS\_pub}$)
8: set *info*, *Flag*=T
9: **else**
10: Random Fill *Data*
11: Set *info*, *Flag*=F
12: **end if**
13: encapsulate, $Pkt = M_{data} \| info$
14: encrypt, *S*=En(*Pkt*, $K_{next}$)
15: send *S* to the next-hop node

We set the network scale as ten hops, so the total number of the nodes in this network is 861; the number of nodes for each hop is given in Table 1. Set the injection rate $\mu = 1$ and $\omega = 16$. First, comparing the sectors number for authentic packets mixing on the mix-ring under different queue lengths (*Length* = 4, 8, 16) and anonymity thresholds (*Anony* = 50, 75, 100 %), the distribution is presented in Fig. 6. And comparing the hops for authentic packets mixing on the mix-ring under different queue lengths (*Length* = 4, 8, 16) and anonymity thresholds (*Anony* = 50, 75, 100 %), the distribution is presented in Fig. 7. It can be inferred from this figure that at same requirement of anonymity degree, with the decrease in queue length, the expectation of the sectors number will increase consistently. This is because that the shorter the queue length is, the less the packets for mixing provided by each node, more nodes need to participate in mixing in order to reach the packet's requirement of anonymity threshold; therefore, more sectors will be required.

Figure 8 illustrates the latency distribution of real data packets mixing on the mix-ring under different thresholds of anonymity and different lengths of queue. Figure 9 illustrates the latency cumulative distribution of real data

**Table 1** The number of nodes for each ring

| Hops | Nodes |
|---|---|
| 1 | 9 |
| 2 | 26 |
| 3 | 43 |
| 4 | 60 |
| 5 | 78 |
| 6 | 95 |
| 7 | 112 |
| 8 | 129 |
| 9 | 146 |
| 10 | 163 |

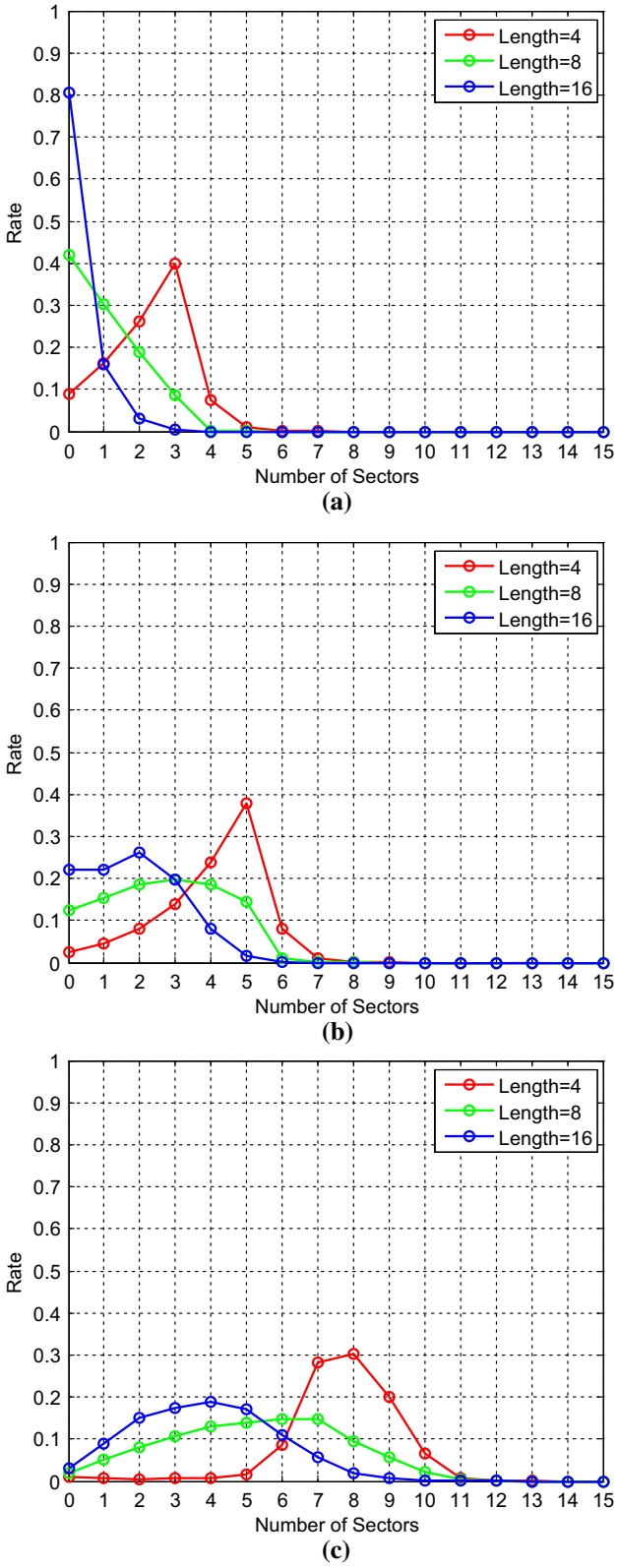



**Fig. 6** The sector number distribution for different queue lengths of authentic packets mixing under different anonymity thresholds. **a** Anonymity threshold = 50 %, **b** anonymity threshold = 75 %, **c** anonymity threshold = 100 %

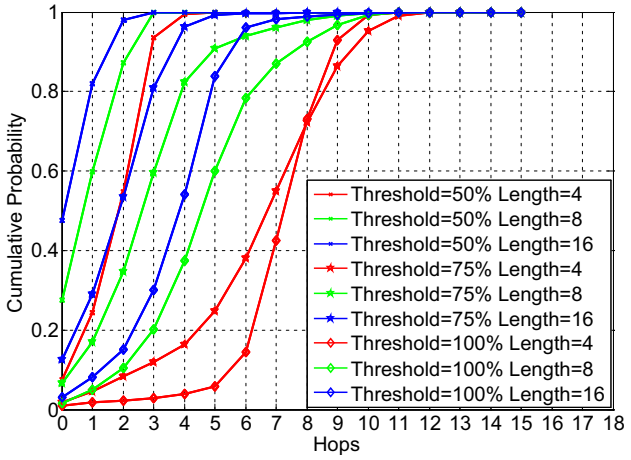



**Fig. 7** Cumulative distribution probability of hops for mixing packets under different thresholds and different lengths

packets mixing on the mix-ring under different thresholds of anonymity and different lengths of queue. As shown in Figs. 8 and 9, the higher the threshold is, the longer the mixing time is under the same queue length because more packets from different quadrants need to be mixed. The longer the queue length is, the longer the mixing time is under the same threshold because the more the number of packets in the queue is, the longer the time expectation of waiting to be sent on each node is.

To examine the corresponding position relationship between authentic packets entering/leaving the mix-ring and leaving after the completion of mixing, the statistical distribution of the sector number for packets leaving the mix-ring which comes from No. 8 sector is shown in Fig. 10. When the queue length is 8 compared with 16 and 4, the curve fluctuations are minimal under different anonymity thresholds, the sectors relationship is unsubstantial between authentic packet entering and leaving the mix-ring, and the probability that the attackers get the packet source-sector through the relationship is the lowest. Therefore, the queue length is set as 8 in the following simulation experiments.

As shown in Fig. 11, we compare the delay condition of sending packets from different rings to the mix-ring under the piggyback mechanism and the common mechanism. The 5th hop is set as the mix-ring. The interval expectation of each node sending a packet is 10 s. In the piggyback mechanism, the real data packets can be replaced by the packets from the upstream when the nodes close to the mix-ring send packets, thus shortening the waiting delay.

In contrast to ordinary injection mechanism, we compare the energy consumption in the same injection interval $\mu = 1$, and the energy consumption distribution when selecting different rings as the mix-ring as well as the energy consumption of Inject protocol. The result is shown in Fig. 12. When a ring is selected as mix-ring, energy consumption peak appears in the ring because mix-ring is

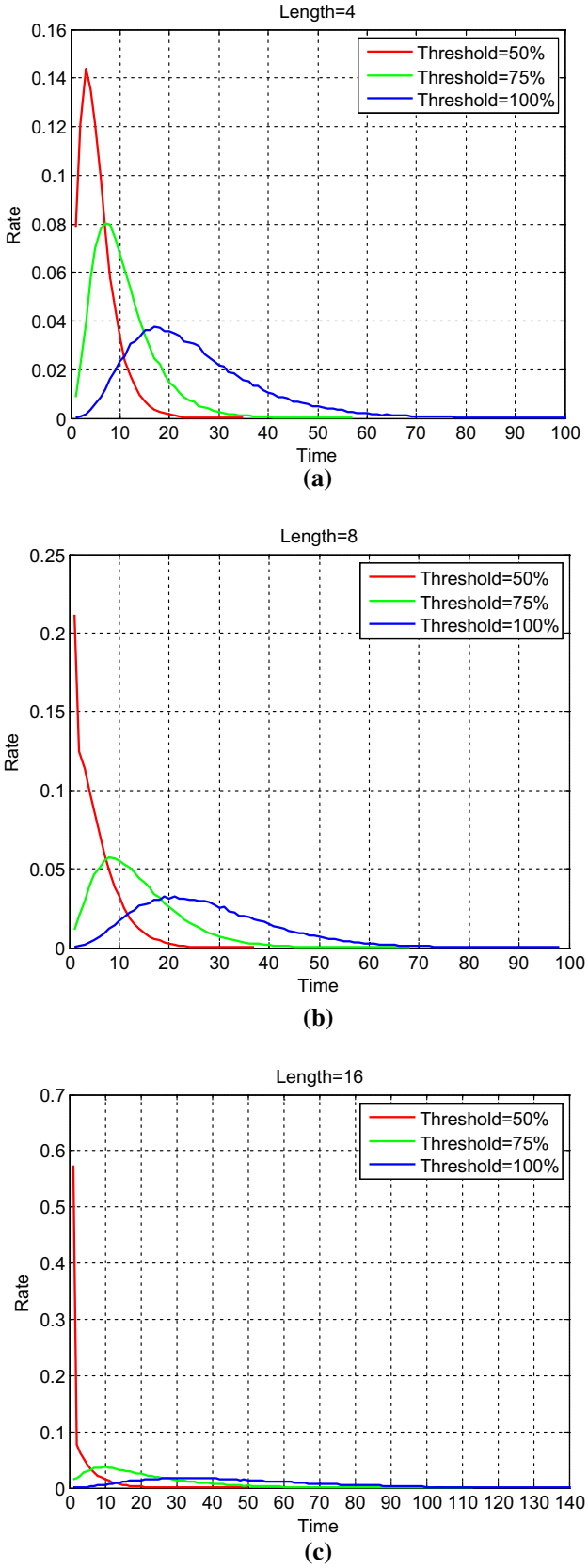
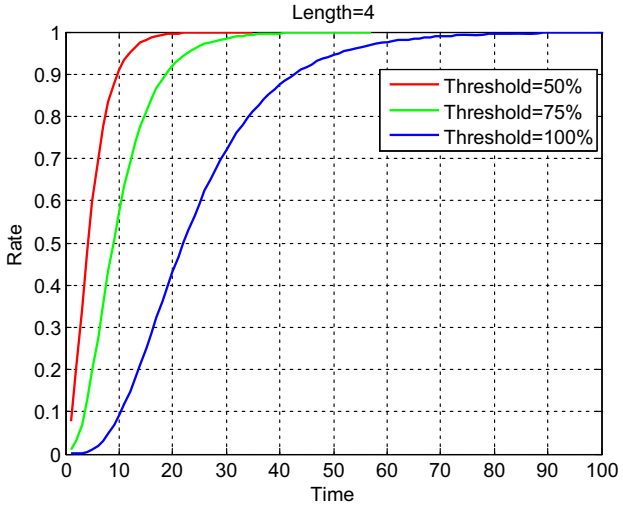
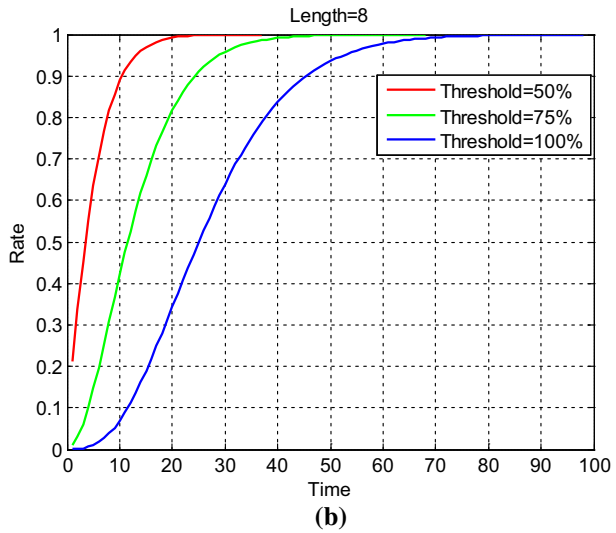


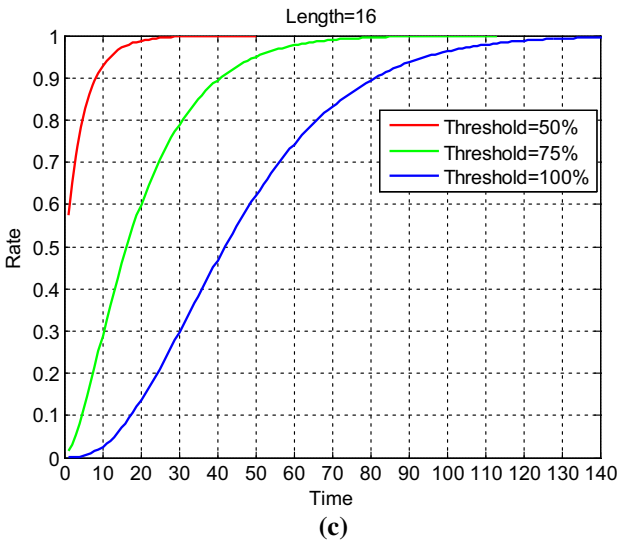

**Fig. 8** Mixing latency distribution for packets which required different degrees of anonymity. **a** *Length* = 4, **b** *length* = 8, **c** *length* = 16




(a)

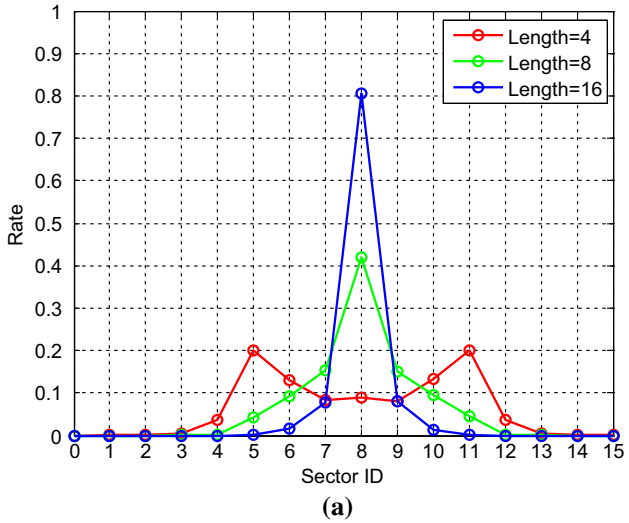



(b)

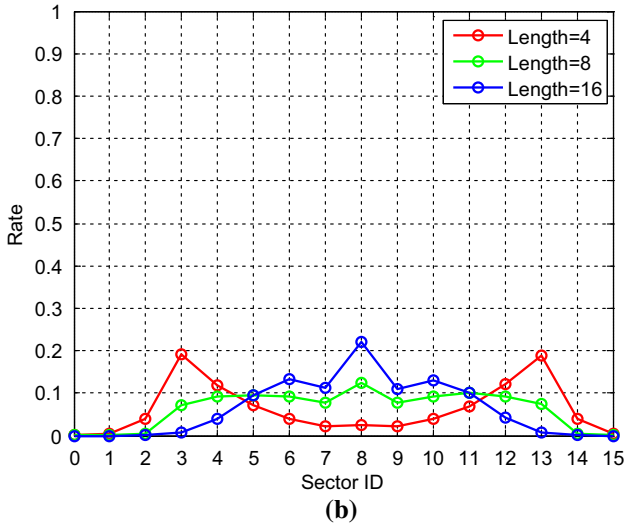



(c)

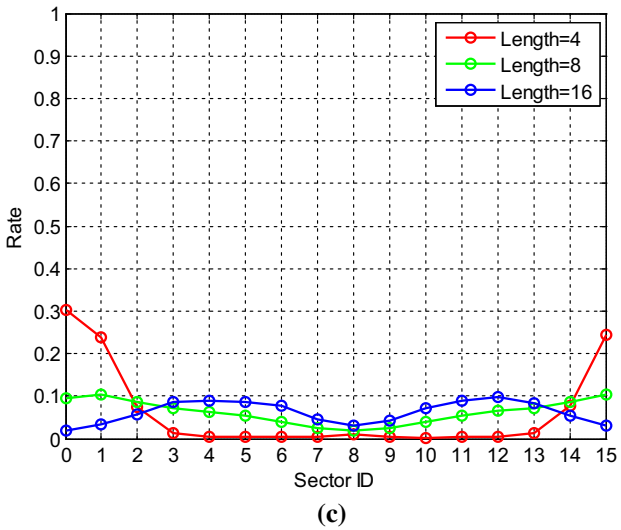
**Fig. 9** Mixing latency cumulative distribution for packets which required different degrees of anonymity. **a** *Length* = 4, **b** *length* = 8, **c** *length* = 16




(a)




(b)




(c)

**Fig. 10** The sector number distribution of authentic packets leaving the mix-ring. **a** *Anony* = 50 %, **b** *anony* = 75 %, **c** *anony* = 100 %

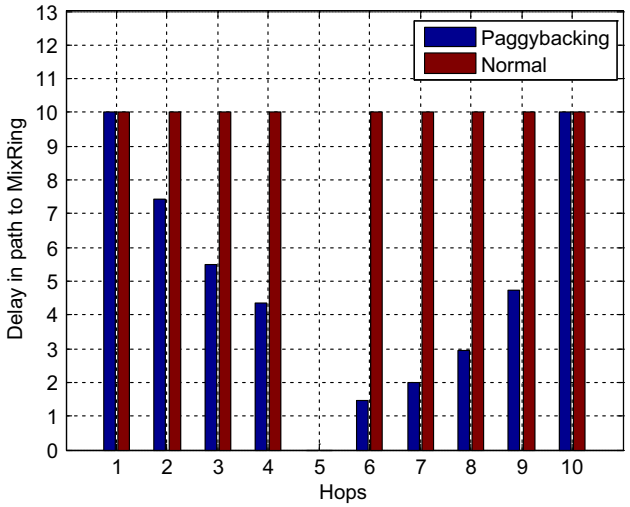



**Fig. 11** Delay of sending real packets from different rings to mix-ring under the piggyback mechanism

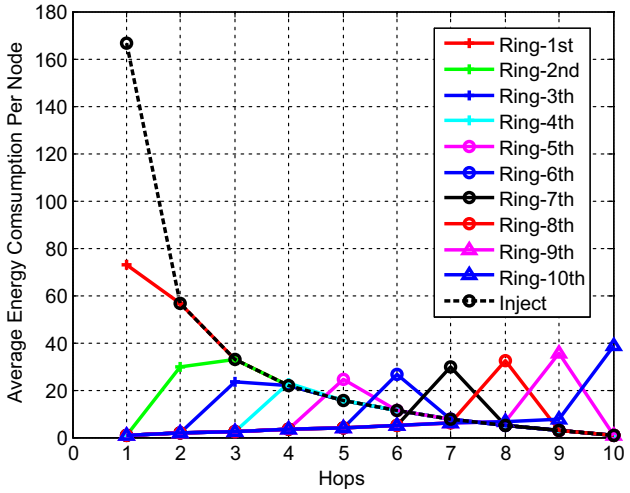



**Fig. 12** Under the circumstance of the network scale is ten hops, the average energy consumption for nodes when choosing different ring as the mix-ring

**Table 2** Time ratio for each ring

| Hops | Time ratio |
|---|---|
| 1 | 0.58 |
| 2 | 0.77 |
| 3 | 0.86 |
| 4 | 0.92 |
| 5 | 0.96 |
| 6 | 0.99 |
| 7 | 1.00 |
| 8 | 1.00 |
| 9 | 0.99 |
| 10 | 0.97 |

responsible for numerous packet retransmissions. By optimizing the energy consumption and making full use of energy, Table 2 shows the optimal energy consumption distribution. Compared with ordinary injection protocol, the lifetime ratio is 1:0.25. As the network scale becomes larger, the "funnel effect" increases sharply in Inject protocol while DORing can optimize the energy consumption. Thus, when network scale is larger, the lifetime of DORing is longer compared with Inject protocol.

### 5.3 Security analysis

**Theorem 1** *In DORing, authentic packets cannot be distinguished from dummy packets.*

*Proof* In the process of packet generation, generation and transmission of authentic packets and dummy packets are subject to the same statistics distribution. Adversaries cannot distinguish authentic packets from dummy one and are unable to locate the event source.

**Theorem 2** *In DORing, authentic packets cannot be traced during the process of transmission.*

*Proof* In the process of packet-confusion in the mix-ring, the SecBit of a packet indicates with which sector of packets it will mix. When reaching 100 % anonymity threshold, packets from all sectors are mixed with the packet. The behaviors of all nodes are the same, which makes authentic packets untraceable. Adversaries cannot trace back to the source node by means of traffic analysis.

Thus, DORing can guarantee the anonymity of source node throughout the entire process from packets generation to base station receiving.

## 6 Conclusions

This paper proposes a dynamic optimal mix-ring-based source-location anonymity protocol for local/global traffic snoop analysis attack, namely DORing. In this protocol, dummy traffic injection is adopted to resist global traffic snoop analysis attack. And mix-ring is utilized to confuse packets, which eliminates the correlation between packets and source node. Authentic packets are separated and the rest of dummy traffic is cut off without compromising source anonymity. The simulation results and security analysis demonstrate that DORing can effectively resist source-location privacy attack with global traffic snoop capability, balance and optimize energy consumption and transmission latency as well as significantly prolong lifetime of the network.

**Acknowledgments** This work was partially supported by the National Key Research Development Program of China (Grant No. 2016YFB0502201), the National Natural Science Foundation of China NSFC (Grant Nos. 41127901-06, 61572370, 61450110441, 61572374, U1135005), Development Program of China "863 Project" (Grant No. 2015AA016004), the Natural Science Foundation of Hubei Province of China (Grant No. 2014CFB191) and the CERNET Next Generation Internet's Technology Innovation Project (NGII20150612).

## References

1. Winkler T, Rinner B et al (2014) Security and privacy protection in visual sensor networks: a survey. ACM Comput Surv (CSUR) 47(1):2–42
2. Sun Y et al (2016) Internet of things and big data analytics for smart and connected communities. IEEE Access 4(2016):766–773
3. Sun Y, Jara AJ (2014) An extensible and active semantic model of information organizing for the internet of things. Pers Ubiquitous Comput (PUC) 18(8):1821–1833
4. Guo J, Sun Y et al (2014) Square-root unscented Kalman filtering-based localization and tracking in the internet of things. Pers Ubiquitous Comput (PUC) 18(4):987–996
5. Long J et al (2015) An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing. J Parallel Distrib Comput 81:47–65
6. Sun Y et al (2014) Data security and privacy in cloud computing. Int J Distrib Sens Netw 2014(190903):1–9
7. Xi Y, Schwiebert L, Shi W (2006) Preserving source location privacy in monitoring-based wireless sensor networks. In: IEEE international parallel and distributed processing symposium (IPDPS 2006), pp 1–8
8. Shaikh RA et al (2010) Achieving network level privacy in wireless sensor networks. Sensors 10(3):1447–1472
9. Akyildiz IF et al (2002) Wireless sensor networks: a survey. Comput Netw 38(4):393–422
10. Conti M, Willemsen J, Crispo B (2013) Providing source location privacy in wireless sensor networks: a survey. IEEE Commun Surv Tutor 15(3):1238–1280
11. Chen H, Lou W (2015) On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. Pervasive Mob Comput (PMC) 16:36–50
12. Li Y, Ren J, Wu J (2012) Quantitative measurement and design of source-location privacy schemes for wireless sensor networks. IEEE Trans Parallel Distrib Syst (TPDS) 23(7):1302–1311
13. Kamat P et al (2005) Enhancing source-Location privacy in sensor network routing. In: IEEE international conference distributed computing systems (ICDCS 2005), pp 599–608
14. Yao L et al (2015) Protecting source–location privacy based on multirings in wireless sensor networks. Concurr Comput Pract Exp 27:3863–3876
15. Ren J, Tang D (2011) Combining source-location privacy and routing efficiency in wireless sensor networks. In: IEEE global telecommunications conference (GLOBECOM 2011), pp 1–5
16. Rios R, Lopez J (2011) Exploiting context-awareness to enhance source-location privacy in wireless sensor networks. Comput J 54(10):1603–1615
17. Lightfoot L, Li Y, Ren J (2010) Preserving source-location privacy in wireless sensor network using STaR routing. In: IEEE global telecommunications conference (GLOBECOM 2010), pp 1–5
18. Yao J, Wen G (2008) Preserving source-location privacy in energy-constrained wireless sensor networks. In: IEEE international conference distributed computing systems (ICDCS2008), pp 412–416
19. Mehta K, Liu D, Wright M (2012) Protecting location privacy in sensor networks against a global eavesdropper. IEEE Trans Mob Comput (TMC) 11(2):320–336
20. Alomair B et al (2013) Toward a statistical framework for source anonymity in sensor networks. IEEE Trans Mob Comput (TMC) 12(2):248–260
21. Shao M et al (2008) towards statistically strong source anonymity for sensor networks. In: IEEE international conference on computer communications (INFOCOM 2008), pp 51–55
22. Zhang Y et al (2010) All proxy scheme for event source anonymity in wireless sensor networks. In: IEEE international conference on intelligent sensors, sensor networks and information processing (ISSNIP 2010), pp 263–268
23. Jhumka A, Bradbury M, Leeke M (2012) Towards understanding source location privacy in wireless sensor networks through fake sources. In: IEEE international conference on trust, security and privacy in computing and communications (TrustCom 2012), pp 760–768
24. Ortolani S et al (2011) Events privacy in WSNs: a new model and its application. In: IEEE international symposium world of wireless, mobile and multimedia networks (WoWMoM 2011), pp 1–9
25. Thomason A et al (2013) Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy. In: IEEE international conference on trust, security and privacy in computing and communications (TrustCom 2013), pp 667–674
26. Mahmoud MM, Shen X (2012) A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. IEEE Trans Parallel Distrib Syst 23(10):1805–1818
27. Mahmoud ME, Shen X (2012) Secure and efficient source location privacy-preserving scheme for wireless sensor networks. In: IEEE international conference on communications (ICC2012), pp 1123–1127
28. Guo M et al (2015) In-network trajectory privacy preservation. ACM Comput Surv (CSUR) 48(2):23–29
29. Roy PK et al (2015) Source location privacy using fake source and phantom routing (FSAPR) technique in wireless sensor networks. Procedia Comput Sci 57:936–941