Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 920510, 14 pages
http://dx.doi.org/10.1155/2014/920510

Research Article

Energy Efficient Source Location Privacy Protecting Scheme in Wireless Sensor Networks Using Ant Colony Optimization

Liming Zhou and Qiaoyan Wen

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Correspondence should be addressed to Liming Zhou; zhouliming1985@gmail.com

Received 2 October 2013; Accepted 17 February 2014; Published 20 March 2014

Academic Editor: Wen-Hwa Liao

Wireless sensor networks consist of various sensors with limited power, which collect different useful and privately relevant information. We pay attention to some issues related to sensor's location privacy. Ant colony optimization provides a natural and intrinsic way of exploration of search space for preserving sensor's location privacy. In this paper, we focus on protecting the sensor's location by introducing suitable modifications to sensor routing to make it difficult for an eavesdropper to find the original location. And we propose an energy efficient preserving sensor's location privacy based on ant colony optimization scheme, which is a flexible routing strategy to protect the sensor's location. Simulation results show that our strategy can efficiently reduce the chance of packets being detected and prolong the network lifetime. And the adversary can find it difficult to find the exact location of the source node.

1. Introduction

Wireless sensor networks have gained more popularity in recent years. In wireless sensor networks, sensors are deployed in various kinds of applications to monitor events and transmit information to base station. In battlefield, sensors are deployed to monitor enemy's activity and send messages to base station. And sensors can also be deployed to monitor the environment and temperature in civilian applications or monitor animals in natural habitats.

In a wireless sensor network, location information often means the physical location of the event, which is crucially given some applications of wireless sensor networks [1]. So if an attacker gets location information by analyzing a message that was captured, he will move to the location and monitor the event. Meanwhile, the attacker will collect a lot of private information. So the information retrieved by these networks is of vital importance and must be properly secured not only from curious eavesdroppers but also from more skilled adversaries. Messages traversing the network can be protected using traditional confidentiality and integrity mechanisms. But, even if an adversary cannot obtain the information contained in the payloads, he can still retrieve other sensitive information by observing and analyzing the communications [2]. For example, an attacker can obtain the information from the network and the environment being monitored by simple observation of the network traffic [3]. Besides, an attacker can compromise users' location privacy by observing the wireless signals from user devices [4, 5].

Although many existing privacy techniques can be employed in sensor network scenarios, they cannot effectively preserve the sensor location in a sensor network [6, 7]. The reason is that the problems are different in fact and many of the methods introduce overhead which are too burdensome for sensor networks. And many techniques do not consider the capacity, computing power, and power of sensors, which are the limiting factors in wireless sensor networks. And some techniques analyze privacy and anonymity issues and propose solutions by manipulating the message contents [8, 9]. In contrast to their schemes, this paper addresses the location privacy threat due to the physical wireless medium that allows the adversary to perform traffic analysis to derive the message flows.

In wireless sensor networks, minimization of energy consumption is considered a major performance criterion to provide maximum network lifetime. Ant colony optimization

algorithms simulating the behavior of ant colony have been successfully applied in many optimization problems such as vehicle routing and the asymmetric traveling salesman as well as routing in wireless sensor networks [10].

In this paper, we preserve sensor location information and prolong the network lifetime in wireless sensor networks. We present an energy efficient source location privacy protecting mechanism (EELP), which applies the ant colony optimization method to protect the location privacy information. Our work differs from previous works. In order to provide strong communication anonymity, a random packet-forwarding strategy is presented. Whenever a node receives a packet, it will figure out the next hop based on the information of the pheromones, the distance, and the remaining energy according to the routing table. Then each node will update the information. After certain rounds of transmissions, procedure of evaporating and depositing pheromones will be applied which help EELP to adjust the amount of the pheromones. So it is unlikely that the adversary will continuously receive event packets from a monitored node because packets are sent through different nodes which can be far from each other. Moreover, even if the adversary could capture the same packet at different relaying nodes, he cannot correlate the packets. When a node sends an event packet, any neighboring node can be the receiver and it is infeasible to figure out the next-hop node. The adversary cannot also infer the direction to the source node by following the movement of the packets because the packets are sent after random delay. A detailed analysis of EELP is provided, and a comprehensive comparison with existing schemes is presented to show its effectiveness and efficiency to preserve sensor location privacy and prolong the network lifetime.

The rest of the paper is organized as follows. Related work and previously proposed techniques for location privacy are presented in Section 2. In Section 3, we illustrate the preliminaries of the paper. After that, Section 4 discusses the system model. Then we present our energy efficient source location privacy protecting scheme in Section 5, followed by the security analysis and performance analysis in Section 6. Section 7 shows the experimental results and their analysis and comparison. Finally, we have the conclusions in Section 8.

2. Related Work

In wireless sensor networks, it is important to provide confidentiality to the sensor's location. In this section, we describe previous proposed technologies that were designed to protect the objects and establish energy efficient topologies to save energy.

For the location information, the periodic collection and the source simulation schemes are proposed in [11], which can protect the source location privacy against the global eavesdropper. In periodic collection method, every sensor node independently and periodically sends packets at a reasonable frequency regardless of whether there are real data to send or not. Although the periodic collection method can efficiently preserve the source location privacy, every sensor node must periodically send data and the method increases the communication overhead and the latency. And in source simulation method, the fake source nodes simulate the real source node to send fake packets. This can confuse the adversary. But there is no balanced energy consumption between nodes.

In order to protect the source location privacy, a cross-layer approach is presented in [12]. This scheme is similar to phantom routing but it hides the walking phase in the MAC layer to prevent the eavesdropper from monitoring messages in the vicinity of the source node. Since beacons are periodically broadcast regardless of the occurrence of real events, the adversary is unable to distinguish legitimate beacons from those containing event data.

ELSP is proposed in [13], which separates the sensor nodes into groups. The source packet is randomly forwarded within and between the groups with elaborate design to ensure communication anonymity. Furthermore, members of each group exchange encrypted traffic of constant packet length to make it difficult for the adversary to trace back. However, the proxy nodes and the key nodes exhaust a lot of energy.

Ren et al. [14] propose a cyclic diversionary routing scheme called CDR. The network is divided into several rings according to the hop counts from the sensors to the sink. And CDR establishes cyclic diversionary route at different levels with a variant probability. When the data package comes to a ring which is scheduled to establish cyclic diversionary route, it will take a round trip and gather data of all the cluster heads in the ring. So this can increase the energy cost of the network.

In order to maximize the time for adversary trace back to source, a parallel-routing protocol is proposed in [15]. The packets from the same source are passed through different paths to the base station. Furthermore, a weighted random stride routing is presented that breaks the entire routing into rounds. In [16], FitProbRate is proposed to maintain source anonymity, which is an exponentially distributed dummy traffic generation scheme. The Fitprob parameter decides the dummy traffic generated at a dynamic rate, which differs from other similar works. It is a great improvement over source simulation and fake sources but still has the drawback of having overhead due to dummy packet generation.

Fan et al. [17] preserve location privacy by using homomorphic encryption operations to prevent traffic analysis in network coding. In [18], each cluster header can filter the dummy packets received from the sensor nodes of its cluster to reduce the number of dummy packets. However, the scheme requires much computation overhead due to using asymmetric-key cryptography, and the packet delivery delay is long because the cluster header sends packets with a fixed rate regardless of the number of events it collects. Mehta et al. [19] formalize the location privacy problem using a global adversary model and compute a lower bound for the overhead required for achieving a given level of privacy protection. The proposed scheme by Alomair et al. [20] can guarantee event indistinguishability by achieving interval indistinguishability, where the adversary cannot distinguish between the first, the middle, or the end of the interval. In [21], dummy packets can be filtered at proxy nodes, and the

lifetime of the WSN is analyzed at different proxy assignment methodologies. Hong et al. [22] propose a scheme that can thwart time correlation attack. In this attack, the adversary exploits the time correlation of transmissions in successive links to learn the end-to-end route. Zhou and Yow [23] propose an anonymous geographic routing algorithm which includes three components to avoid the explicit exposure of identity and location in communication.

In energy-constrained wireless sensor networks, energy efficiency is critical for prolonging the network lifetime. A family of ant colony algorithms called DAACA is proposed in [24]. DAACA consists of three phases: initialization, packets transmissions, and operations on pheromones. In the transmission phase, each node estimates the remaining energy and the amount of pheromones of neighbor nodes to compute the probabilities for dynamically selecting the next hop. After certain rounds of transmissions, the pheromones adjustments are performed, which take the advantages of both global and local merits for evaporating or depositing pheromones. Four different pheromones adjustment strategies which constitute DAACA family are designed to prolong the network lifetime.

In [10], the author wanted to maintain network life time at a maximum, while discovering the shortest paths from the source nodes to the base node using a swarm intelligence-based optimization technique called ACO. A multipath data transfer is also accomplished to provide reliable network operations, while considering the energy levels of the nodes. The energy efficient ant-based routing algorithm for WSNs (EEABR) is proposed in [25], which is another proposed ant-based algorithm to maximize the lifetime of WSNs. The algorithm uses a good strategy considering energy levels of the nodes and the lengths of the routed paths.

3. Ant Colony Optimization Algorithm

3.1. Ant Colony Optimization. In the ACO-based approach, each ant k tries to find a path to provide minimum cost in the network. Ants are launched from a source node s and move through neighbor repeater nodes r_i and reach a final destination node (sink) d. Whenever, a node transmits a data to the destination which is described as a sink or base station, launching of the ants is performed. After launching, the choice of the next node r is made according to a probabilistic decision rule as

$$P_k(r,s) = \begin{cases} \dfrac{[\tau(r,s)]^{\alpha} \cdot [\eta(r,s)]^{\beta}}{\sum_{r \in R_s} [\tau(r,s)]^{\alpha} \cdot [\eta(r,s)]^{\beta}}, & \text{if } k \notin \text{tabu}^r, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where $\tau(r,s)$ is the pheromone value, $\eta(r,s)$ is the value of the heuristic related to energy, and R_s is a set of the receiver nodes. For node r, tabu^r is the list of identities of received data packages previously. α and β are two parameters that control the relative weight of the pheromone trail and heuristic value. Pheromone trails are connected to arcs. Each arc(r,s) has a trail value $\tau(r,s) \in [0,1]$. Since the destination is a stable base station, the last node of the path is the same for each ant travel. The heuristic value of the node r is expressed by

$$\eta(r,s) = \frac{(E_I - E_r)^{-1}}{\sum_{n \in R_s} (E_I - E_n)^{-1}}, \tag{2}$$

where E_I is the initial energy and E_r is the current energy level of receiver node r. This enables decision making according to neighbor nodes' energy levels, meaning that if a node has a lower energy source then it has lower probability to be chosen. Nodes inform their neighbors about their energy levels when they sense any change in their energy levels.

In traditional ACO, a special memory named M_k is held in the memory of an ant to retain the places visited by that ant (which represent nodes in WSNs). In (1), the identities of ants (as sequence numbers) that visited the node previously are kept in the node's memories, instead of keeping node identities in ant's memories, so there is no need to carry M_k lists in packets during transmission. This approach decreases the size of the data to be transmitted and saves energy. In (1) each receiver node decides whether to accept the upcoming packet of ant k or not, by checking its tabu list. So the receiver node r has a choice about completing the receiving process by listening and buffering the entire packet. If the receiver node has received the packet earlier, it informs the transmitter node by issuing an ignore message and switches itself to idle mode until a new packet arrives.

After all ants have completed their tour, each ant k deposits a quantity of pheromone $\Delta\tau^k(t)$ given in (3), where $J_w^k(t)$ is the length of tour $w^k(t)$, which is done by ant k at iteration t. The amount of pheromone at each connection $(l(r,s))$ of the nodes is given in (4). In WSNs, $J_w^k(t)$ represents the total number of nodes visited by ant k of tour w at iteration t:

$$\Delta\tau^k(t) = \frac{1}{J_w^k(t)}, \tag{3}$$

$$\begin{aligned} \tau(r,s)(t) &\longleftarrow \tau(r,s)(t) + \Delta\tau(r,s)(t), \\ \forall l(r,s) &\in w^k(t), \quad k = 1, 2, \ldots, m. \end{aligned} \tag{4}$$

Pheromone values are stored in a node's memory. Each node has information about the amount of pheromone on the paths to their neighbor nodes. After each tour, an amount of pheromone trail $\Delta\tau^k$ is added to the path visited by ant k. This amount is the same for each arc(r,s) visited on this path. This task is performed by sending ant k back to its source node from the base along the same path, while transferring an acknowledgement signal for the associated data package. Increasing pheromone amounts on the paths according to lengths of tours, $J_w(t)$, would continuously cause an increasing positive feedback. In order to control the operation, a negative feedback, the operation of pheromone evaporation after the tour, is also accomplished in (5). A control coefficient $\rho \in (0,1)$ is used to determine the weight of evaporation for each tour [10]:

$$\tau_{ij}(t) \longleftarrow (1-\rho)\,\tau_{ij}(t). \tag{5}$$

Table 1: Energy parameters table.

Symbol	Definition	Values
$E_{\text{Tx-elec}}$	Transmitter electronics	50 nJ/bit
$E_{\text{Rx-elec}}$	Receiver electronics	50 nJ/bit
ε_{amp}	Transmit amplifier	100 pJ/bit/m^2

In simulations, ACO parameter settings are set to values 1 for α, 5 for β, and 0.5 for ρ, which were experimentally found to be good by Dorigo [26].

3.2. Energy Consumption Model. Many energy models [27, 28] are used for energy consumption in wireless sensor networks. In our work, we employ the model in which a packet with the size k_s to be transmitted in the distance of d will consume

$$E_{\text{Tx}}(k_s, d) = E_{\text{Tx-elec}} \times k_s + \varepsilon_{\text{amp}} \times k_s \times d^2 \quad (6)$$

for the transmitter and

$$E_{\text{Rx}}(k_s) = E_{\text{Rx-elec}} \times k_s \quad (7)$$

for the receiver, respectively. The definitions of the symbols are listed in Table 1.

4. System Model and Design Goals

4.1. Network Model. Sensor networks consist of a number of different types of sensor nodes that have been deployed to monitor environment or collect data and send information to the sink in an area. In sensor networks, every sensor sends data to its neighboring nodes within its radio range.

In this paper, we assume that sensor nodes are evenly deployed in the sensor network and do not move after being deployed. All of sensors have roughly the same capabilities, power sources, and expected lifetimes. When a sensor node monitors an object, the node will send a message to a base station. And a message is forwarded through certain routing strategies that adopted the sensor networks. Moreover, we assume that a base station is deployed in the network and collects event data with greater computational capabilities.

4.2. Adversary Model. For various kinds of wireless sensor networks, we assume that an adversary is a motivated and funded attacker whose objective is to learn sensitive location-based information. The adversary has unbounded energy resource, adequate computation capability, and sufficient memory for data storage. And the adversary can observe and eavesdrop on the information in a limited range. Although the adversary can eavesdrop on the message between nearby sensor nodes to backtrace to a parent node, the adversary cannot determine the content of the message that is encrypted by secret keys.

Similar to [29], we assume that the adversary stays nearby the base station or the sink, where it is guaranteed that a large number of packets will arrive eventually. The adversary is constantly monitoring and eavesdropping. When the eavesdropper monitors a message, he knows which node among the neighborhood sent that message and will move to the transmitting node. If the eavesdropper does not monitor any message for a certain time, he will stay or go back one step and keep monitoring. The adversary repeats this process until it reaches the source. Then the adversary can know the location information of source node. Besides, the adversary can monitor the different transmission rates between the nodes and select the correct backtracking routing. And the eavesdropper may observe the correlation in transmission times between a node and its neighbor, attempting to deduce a routing path.

4.3. Design Goals. The network is modeled as a visibility graph $G = (V, E)$, where V is the set of sensor nodes. Each node has the maximum transmission range denoted by R, by which it can setup its neighbor set and routing table. e_{ij} represents the distance between node i and node j which is smaller than R; meanwhile, the neighbor set $\Omega(i)$ of node i indicates a set of nodes whose distances are less than R ($\Omega(i) = \{j \mid e_{ij} \leq R\}$). The set of e_{ij} comprises the E. The goal is to find an energy efficient routing path to prolong the network lifetime and prevent the adversary from getting the source information by analyzing the traffic pattern.

5. The Energy Efficient Location Privacy Protecting Scheme

In this section, we propose EELP family to protect location privacy. In EELP family, we choose different process of evaporating and depositing pheromones to prevent the adversary from getting the location information. We first give the basic idea of the energy efficient location privacy protecting scheme (EELP), and then two heuristic algorithms (LRP-EELP, LPU-EELP) are proposed to enhance the basic idea. In Section 5.1 we present the basic idea of EELP, LRP-EELP is shown in Section 5.2, and Section 5.3 describes LPU-EELP in detail, respectively. And we assume that the contents of all transmitted data packets are encrypted by secret keys so that the adversary cannot gain the content of transmitted packets and find the location of sensors. Many key predistribution protocols can be used for our purpose [30–32]. So the adversary cannot use the content to trace the object.

5.1. The Basic Idea of EELP. In wireless sensor network, nodes are considered as the artificial ants. The routing table records the amount of the pheromones of links. Whenever a node receives a packet, it will figure out the next hop based on the information of the pheromones, the distance, and the remaining energy according to the routing table. Then each node will update the information. After certain rounds of transmissions, procedure of evaporating and depositing pheromones will be applied which help EELP to adjust the amount of the pheromones. The objective of this process is to guide the transmitting routing path to approach the global optimal routing path which will conserve energy for the network to some extent.

Firstly every node constructs its own neighbor set and routing table by broadcasting its *id* and location information within R. Afterwards, the transmission process starts. Packets are transmitted from the source nodes to the sink node in each round. When a node receives a packet, it will evaluate contents of the routing table including the remaining energies and the amount of pheromones to calculate the transmission probabilities of selecting the next hop. Then one of its neighbors will be selected. When the number of round is equal to the *updateRound*, all nodes will perform the evaporating and depositing operations. Each node evaporates the pheromones of its neighbor and deposits pheromones according to different specific conditions. After that each node will update the pheromones of its neighbors.

The structure of EELP is shown in Algorithm 1. Initially, the initialization of the network is carried out. Each node broadcasts "*Init*" message to its neighbors. Then only the nodes that are nearer to the sink node will be recorded in the routing table and the contents of the table are initialized. Then the transmission begins, the source nodes periodically send the data packets to the sink node. When a relay node receives a packet, it will calculate the probability of selecting the next hop based on the elements in the routing table including the distance, the amount of the pheromones, and the estimated remaining energy. The transmission proceeds until the data are transmitted to the sink node. After transmitting *updateRound* rounds, adjustments of pheromones are carried out. Each node updates the routing table to keep the information fresh. At last each node broadcasts its actual energy, by which the neighbor nodes will update the contents of the routing table.

In the EELP, the pheromone is the most critical part in adjusting the probabilities in the routing table. Therefore, we firstly illustrate the constitution of the routing table. The routing table contains the following elements: $\{\text{id}, p(i,j), \tau(i,j), E_{\text{est}}(i,j), E_\eta(i,j)\}$, and $j \in \Omega(i)$; id is the identity of the node. $p(i,j)$ is the probability for node i to select node j as the next hop which is computed as follows:

$$p(i,j) = \frac{[\tau(i,j)]^\alpha \cdot [\eta(i,j)]^\beta}{\sum_{j\in\Omega(i)} [\tau(i,j)]^\alpha \cdot [\eta(i,j)]^\beta}. \tag{8}$$

α and β are two parameters which control the relative weight of the pheromone $\tau(i,j)$ and heuristic value $\eta(i,j)$. $\eta(i,j)$ represents the inverse value of the energy distance $E_\eta(i,j)$ between nodes i and j, which is given by

$$\eta(i,j) = \frac{1}{E_\eta(i,j)}. \tag{9}$$

$E_\eta(i,j)$ can be calculated as

$$E_\eta(i,j) = \frac{E_{\text{dis}}(i,j)}{e_1(i) \times e_2(i,j)} \quad (0 < e_1 < 1,\ 0 < e_2 < 1), \tag{10}$$

where

$$e_1(i) = \frac{E_{\text{cur}}(i)}{E_{\text{init}}}$$
$$e_2(i,j) = \frac{E_{\text{est}}(i,j)}{E_{\text{init}}}. \tag{11}$$

$E_{\text{cur}}(i)$ is the current energy of node i. $E_{\text{dis}}(i,j)$ is the energy distance which can be given by

$$E_{\text{dis}}(i,j) = E_{Tx\text{-elec}} \times k_s + \varepsilon_{\text{amp}} \times k_s \times e_{ij}^2. \tag{12}$$

k_s is the size of the packet. $E_{\text{est}}(i,j)$ shows the energy of node j estimated by node i, which can be estimated as follows:

$$E_{\text{est}}(i,j) = E_{\text{init}} - \frac{E_{\text{init}} - E_{\text{est}}(i,j)}{T(i,j)} \times [T(i,j) + 1]. \tag{13}$$

$T(i,j)$ is the transmission times from node i to node j.

In the transmission phase, when a node receives a packet, it will evaluate the remaining energy of all the neighbors and update all the values in the routing table to dynamically select the next hop. When round is multiple of *updateRound*, procedure adjusting the pheromones starts. First, the pheromones should be evaporated according to

$$\tau(i,j) = (1-\rho) \times \tau(i,j). \tag{14}$$

ρ stands for the rate of evaporating pheromones. Then the procedure of depositing pheromones is performed. Each node selects the neighbor with the maximum estimation energy (e.g., the node j) and increases the pheromone of node j by $E_{\text{dis}}(i,j)$ as

$$\tau(i,j) = \tau(i,j) + E_{\text{dis}}(i,j). \tag{15}$$

When round is multiple of *updateRound*, Algorithm 2 is called to adjust the pheromones for each node. Firstly, the evaporating and depositing of pheromones are taken. Then updating of the routing table is carried out.

Once Algorithm 2 is finished, in the next period of *updateRound*, the node with the highest $E_{\text{dis}}(i,j)$ will have a higher probability of being selected as the next hop. After finishing depositing pheromones, the process of updating the estimated energy value is performed. Each node will broadcast its current energy in the range of R. The value of $E_{\text{est}}(i,j)$ will be updated.

If a node happens to exist in the conjunction of two or more different paths, the parent nodes will also use (15) to increase the pheromones.

5.2. The Limited Range of The Pheromones-Based EELP. In order to protect the location privacy, we require that the packets are randomly transmitted to the sink according to the pheromones. We use $[\tau_{\min}, \tau_{\max}]$ to limit the range of the pheromones called LRP-EELP. The reason is that if the pheromone is not limited in a range, some paths will own higher probabilities than the others; nevertheless, with the transmission going on, nodes in this kind of path will cost

```
(1) Network Initialization
    Node Initialization
    Neighbor Initialization
    Routing Table Initialization
(2) The source node begin to send its data packets to the destination hop by hop
(3) for all nodes i are the neighbors of the node s do
(4)     the node s evaluates the energy of i.
(5)     the node s calculates p(s, i).
(6)     the node s selects the next hop node k based on p(s, k) (i = k).
(7) end for
(8) the node s sends the packets to the node k
(9) while the node s is not the sink do
(10)    for all nodes j are the neighbors of the node k do
(11)        the node k evaluates the energy of j.
(12)        the node k evaluates p(k, j).
(13)        the node k selects the next hop node g based on p(k, g) (j = g).
(14)    end for
(15)    the node k sends the packets to the node g
(16) end while
(17) round = round + 1
(18) if round = updateRound then
(19)    Evaporating Pheromones.
(20)    Depositing Pheromones.
(21)    Updating Routing Table.
(22)    Energy Broadcasting.
(23) end if
```

Algorithm 1: EELP structure.

```
(1) for all nodes i do
(2)   the node i evaporates the pheromones.
(3)   the node i searches for the node with the highest E_est(i, j) where j ∈ Ω(i) in neighbor set.
(4)   the node i deposits pheromones
(5)   if the conjunction times of node i ≥ 2 then
(6)     for all nodes j are the neighbors of the node i do
(7)       j deposits pheromones of i according to (15).
(8)       i broadcasts the current energy.
(9)     end for
(10)  end if
(11)  if the node i receives a broadcast message from j then
(12)    the node i updates E_est(i, j).
(13)    the node i updates the routing table.
(14)  end if
(15) end for
```

Algorithm 2: Adjusting pheromones of EELP.

more energy than the others. And the adversaries can easily backtrace to the source node. But according to (8), the amount of pheromones is still large, which may cause them more likely to be selected as the next hop and ultimately results in local optimal solution. However, if the constraints of pheromones are imposed, the aforementioned phenomenon can be avoided and variety of paths will be formed; hence, it is efficient to prevent the adversary to backtrace to the source node and prolong the network lifetime.

We set the format of the packet header, which obtains the id sequence of nodes and total energy consumption as $\mathrm{ID}_{\mathrm{list}}$ and $E_{\mathrm{consumption}}$. $\mathrm{ID}_{\mathrm{list}}$ includes all the nodes in the trace from the source to the current node. $E_{\mathrm{consumption}}$ is defined as the total transmission energy cost from the source to the current node.

When a packet is received by a node, it will be taken which adds id information and energy consumption information into the newly defined packet header. And the sink node can gain the energy cost of the transmission path and adjust the amount of pheromones to obtain more transmission paths. Let E_{cost} be the minimum energy cost in a transmission path.

When a packet is sent to the sink node, the sink node checks if the $E_{\mathrm{consumption}}$ is smaller than E_{cost}, if so, the E_{cost} and the corresponding $\mathrm{ID}_{\mathrm{list}}$ will be updated. When round is

multiple of *updateRound*, the sink node will perform global deposition process. Each node in the $\mathrm{ID}_{\mathrm{list}}$ will update the pheromones as follows:

$$\tau(i,j) = \begin{cases} \tau_{\min}, & \tau(i,j) \le \tau_{\min} \\ (1-\rho)\cdot\tau(i,j) + \rho\cdot\dfrac{1}{E_{\mathrm{cost}}}, & \tau_{\min} \le \tau(i,j) \le \tau_{\max} \\ \tau_{\max}, & \tau(i,j) > \tau_{\max} \end{cases} \quad \left(j \in \Omega(i), i \in P_{\min}, j \in P_{\min}\right), \tag{16}$$

where $P_{\min}$ is the minimum energy cost path.

5.3. The Local Pheromones Updating-Based EELP. According to [33], Ant Colony System (ACS) applies the mechanisms of ACO but some changes have been made to overcome the drawbacks of ACO and enhance the performance of ACO. ACS can make full use of the accumulated pheromones in the path. And the evaporating and releasing of the pheromones are only carried out in the most optimal path so far. When an ant passes through a trail, the pheromone of that trail will be reduced which aims at enhancing the possibility of finding more optimal solutions in other trails.

We use the Ant Colony System-based EELP algorithm for establishing the location privacy protecting paths to preserve energy called LPU-EELP. When a node selects the next hop node, we set a random parameter $q_0 \in [0,1]$. The node i selects the next hop node j as

$$j = \begin{cases} \arg\max\limits_{j\in\text{allowed}} \left\{\tau(i,j)^{\alpha} \times \eta(i,j)^{\beta}\right\}, & q \le q_0 \\ (8), & q > q_0, \end{cases} \tag{17}$$

where allowed is the set of the unselected nodes.

After successfully sending the packet in each round, each node will locally update the pheromones as follows:

$$\tau(i,j) = (1-\rho)\times\tau(i,j) + \rho\times\Delta\tau(i,j). \tag{18}$$

ρ stands for the rate of evaporating pheromones and

$$\Delta\tau(i,j) = \min_{j\in\Omega(i)}\left(\tau(i,j)\right). \tag{19}$$

The local pheromones updating aims at reducing the probability of the selected node; thus, the probabilities of unselected nodes will increase. So this can prevent the adversary from getting the source information by analyzing the traffic pattern.

6. Performance Analysis

In this section, we will analyze the source location privacy of the proposed routing scheme. And then we will give the analysis of the communication overhead of EELP. Finally, we make an evaluation of the trace back time. From the following analysis, we can see that our scheme brings a better network security and maximal network lifetime.

6.1. Security Analysis. In EELP, the contents of all transmitted data packets are encrypted by secret keys so that the adversary cannot gain the content of transmitted packets and find the location of sensors. So the adversary cannot use the content to trace the object. And we assume that the adversary monitors a local area with the intention of locating objects. We describe that a node i transmits a packet which is observed by the adversary at time t. And each observation is a tuple (i,t). Let G_T be all observation collected by the adversary.

The adversary wants to identify a set $D_T \subset I$ of nodes which represent the set of possible locations in the local network. So the adversary knows that the monitoring objects are close to some nodes in D_T at time T. Meanwhile, he will believe that another node transmits a packet to the node. So there is a transmitting path which is a set of observations during the lifetime of the network upto time T. Obviously, for each $i \in D_T$, there must exit a set $W_i \subset G_T$ that can be generated by an object. We call each such set of observations a possibility trace. In other words, a possibility trace is any subset of the adversary's observations that could be the transmitted result of a packet.

There is a close relationship between the location privacy and the analysis of location information of the adversary. The more uncertainty the adversary will analyze the location of nodes, the better protecting location privacy is. In the eavesdropping area, the adversary will need to choose the nodes of his analysis. We assume that the possible sensor nodes in D_T include real nodes which transmit data to sink. So if the size of D_T is very large, the adversary will find it difficult to gain the accurate location information. In other words, it is good for protecting location privacy. Let D_R be the set of the protected nodes. We use information-theoretic metric called entropy [34], to measure the privacy protection provided by our scheme. The entropy of identifying the real source node in the wireless sensor network is defined as

$$c = -\sum_{i=1}^{|D_T|} P_i \cdot \log_2(P_i), \tag{20}$$

where P_i is the probability that node i is the source node, $|D_T|$ is the number of nodes that is uncertain by the adversary, and $\sum_{i=1}^{|D_t|} P_i = 1$. Therefore, the probability P_i of any sensor nodes in D_T being real nodes can be estimated by $|D_R|/|D_T|$. Then we denote the size of D_T as M ($|D_T| = M$). And let m be the size of the protected nodes set ($|D_R| = m$). And we define the location privacy as

$$\begin{aligned} c &= -\sum_{i=1}^{|D_T|} \frac{|D_R|}{|D_T|} \cdot \log_2\left(\frac{|D_R|}{|D_T|}\right) \\ &= -\sum_{i=1}^{M} \frac{m}{M} \cdot \log_2\left(\frac{m}{M}\right) \\ &= m \cdot \log_2\left(\frac{M}{m}\right). \end{aligned} \tag{21}$$

The entropy characterizes the adversary's uncertainty about the location of the source node in a wireless sensor network. The maximum entropy (or the maximum privacy

level) can be achieved when the probabilities P_i pursue uniform distribution, that is, when the adversary believes that all the nodes in the network have the same probability to be the real source node. So we define set $D_T^* = I$, where I is the set of nodes in the whole sensor network. And $|I| = N$, where N is the number of nodes in the whole network.

In this case, the source node is perfectly hidden in the network and the adversary cannot reduce the anonymity set. Therefore, we have the optimal entropy

$$\begin{aligned} c &= -\sum_{i=1}^{|D_T|} \frac{|D_R|}{|D_T|} \cdot \log_2 \left(\frac{|D_R|}{|D_T|} \right) \\ &= |D_R| \cdot \log_2 \left(\frac{|D_T|}{|D_R|} \right) \\ &\leq |D_R| \cdot \log_2 \left(\frac{|D_T^*|}{|D_R|} \right) \\ &= m \cdot \log_2 \left(\frac{N}{m} \right). \end{aligned} \tag{22}$$

We note that the level of location privacy is measured by the size of D_T and D_R. In different applications and context, the privacy measurement can be modified for different privacy requirements.

We note that the size of D_T can influence the level of location privacy. In other words, if the adversary gains certain location information and monitor a particular trace, the privacy would go lower. However, the privacy can increase if the number of the possible traces increases. Above this depends on the sensor network application and the adversary model. For instance, if the adversary wants to identify the location of certain nodes, spending a lot of time to investigate the possible locations, the privacy can be preserved and the location information can be security at any time before T. At each point in time, we can get the appropriate level of location privacy for different context.

For packet back tracing attack, it is unlikely that the adversary will continuously receive event packets from a monitored node because packets are sent through different nodes which can be far from each other. Moreover, even if the adversary could capture the same packet at different relaying nodes, he cannot correlate the packets. When a node sends an event packet, any neighboring node can be the receiver and it is infeasible to figure out the next-hop node. The adversary cannot also infer the direction to the source node by following the movement of the packets because the packets are sent after random delay.

6.2. Communication Cost and Privacy. While we preserve the location privacy in the sensor network, we are interested in minimizing the amount of communication overhead. It is efficient to extend the lifetime of sensor network by decreasing the communication overhead. Let X_T be a random value that represents the number of observations by time T. And let $E(X_T) = \varepsilon_T$ be the number of transmitted packets by time T. For a given sensor node $j \in D_T$, with corresponding possibility trace W_j, we will have

$$E\left(\left|W_j\right|\right) = E\left(X_T\right) = \varepsilon_T. \tag{23}$$

Theorem 1. *Given a possibility set $D_T = (d_1, \ldots, d_k)$, for any $d_i \in D_T$, let W_i be the corresponding possibility trace. Suppose that p is the probability of an observation being included in another possibility trace. And let c be the level of privacy. Therefore, the minimum communication cost is*

$$\operatorname{Min}\left(E_T\right) = \frac{2^{c/m} \cdot m \cdot \varepsilon_T}{p \cdot \left(2^{c/m} \cdot m - 1\right) + 1}. \tag{24}$$

Proof. For a possibility set $D_T = \{d_1, \ldots, d_k\}$, we have $c = m \cdot \log_2 k/m$ and thus $k = 2^{c/m} \cdot m$. For any $d_i \in D_T$, W_i is a corresponding possibility trace. We have $W = \bigcup_{i=1}^{k} W_i$. So we note that the communication cost at time T can be estimated by $|W|$. Then the probability p represents an observation in another possibility trace. Let E_T be the sum of the communication cost of each possibility trace by time T. We can get the minimum communication cost

$$\begin{aligned} \operatorname{Min}\left(E_T\right) = E\left(|W|\right) &= \frac{\sum_{i=1}^{k} E\left(\left|W_i\right|\right)}{(k-1) \cdot p + 1} \\ &= \frac{k \cdot \varepsilon_T}{\left(2^{c/m} \cdot m - 1\right) \cdot p + 1} \\ &= \frac{2^{c/m} \cdot m \cdot \varepsilon_T}{\left(2^{c/m} \cdot m - 1\right) \cdot p + 1}. \end{aligned} \tag{25}$$

We can get the relationship between privacy and communication cost from Theorem 1. Meanwhile, in order to get the minimum communication cost in the sensor network, we need to achieve a given level of location privacy. If the size of the set D_T is increased in a large sensor network, the number of the possibility traces also grows and p is usually very small. In optimal solution, when D_T is too large, p can be approximated by zero and the communication cost E_T becomes $2^{c/m} \cdot m \cdot \varepsilon_T$. □

Figures 1 and 2 show the relationship between the level of privacy and communication cost. Figure 1 shows the relationship with the different number of protected nodes. For the same p, we can see that as the number of protected nodes (m) increases, increasing the level of privacy require less communication overhead. This is due to the increased number of protected nodes in the same area. The probability that the adversary finds the protected nodes increases. So the communication overhead decreases. When m is low, increasing the level of privacy is needed to increase communication overhead.

In Figure 2, when p increases, the location of nodes is more possible in another trace and the higher level of privacy is needed to generate less communication overhead. When p decreases, we note that an observation belongs to only a few traces, so an observation is in another trace with less possibility. So increasing privacy is needed to generate increasing communication cost.

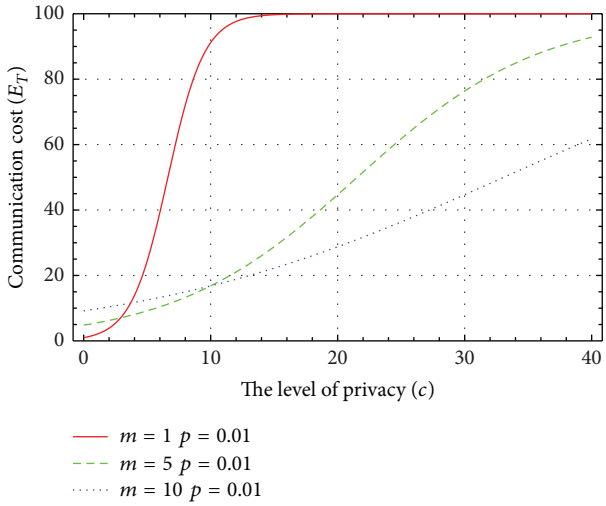

Figure 1: The different number of protected nodes.

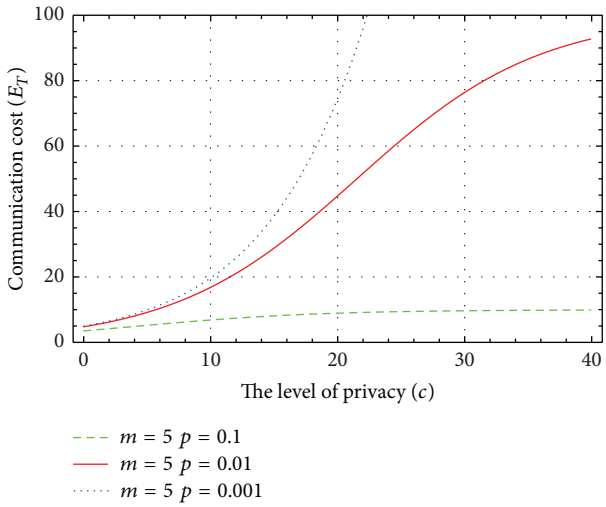

Figure 2: The different probabilities p.

6.3. Trace back Time. In order to preserve location privacy, we analyze the adversary trace back time. If we can increase the trace back time, we can efficiently protect the location information and the adversary may spend lots of time to choose the correct routing. In our scheme we note that sensor nodes can randomly choose their neighbors to transmit a packet to the base station. So this can generate n paths as a set $K_R = \{k_1, k_2, \ldots, k_n\}$ by the real source node in our routing scenario. And the length of each path is the number of hops between the source node and the base station. Let E be the amount of energy required to transmit a packet from the source node to the base station. Then we define the length of each path k_i ($k_i \in K_R$) that can be chosen between k_0 and k_n ($|k_i| \in [k_0, k_n], 1 \le i \le n, E \le k_N$). And we assume that each source node i can randomly choose each path k_i with probability $p_i (p_1 + p_2 + \cdots + p_n = 1)$. Once the adversary starts tracing on one routing path, he will not be able to monitor the packet on the other path. When the adversary eavesdrops the packet on path k_i, the trace back time is $|k_i|/p_i$. We will get the trace back time

$$\begin{aligned} T_{\text{tr}} &= p_1 \cdot \frac{|k_1|}{p_1} + p_2 \cdot \frac{|k_2|}{p_2} + \cdots + p_n \cdot \frac{|k_n|}{p_n} \\ &= |k_1| + |k_2| + \cdots + |k_n| \\ &\le E + (n-1) \cdot k_N. \end{aligned} \tag{26}$$

We note that when all of the flows are distributed to k_1 and all other paths have the maximum length, the average trace back time is maximized.

7. Experimental Results

In this section, we simulate different algorithms (CDR, ELSP, EELP, LRP-EELP, and LPU-EELP) to evaluate and compare the performances of the EELP family with existing schemes. We analyze the energy cost of each node and the network lifetime. Meanwhile, we evaluate the network security and location privacy against the adversary attack. In the experiments, our method can effectively preserve the location privacy of sensor node and decrease the communication overhead.

7.1. Simulation Setup. The simulation is based on TOSSIM [35]. In the simulation, we assume that there are sensor nodes distributed randomly in a square area of 100 m × 100 m. All nodes have the same transmission range. The simulation parameters are given in Table 2. There is a single sink node located at center of the wireless sensor networks, which receives the data of source nodes for all the simulations. We use the energy model to estimate the power consumption. After the sensor network is deployed, every node constructs its own neighbor set and routing table by broadcasting its *id* and location information within R. When a node receives a packet, it will evaluate contents of the routing table including the remaining energy and the amount of pheromones to calculate the transmission probabilities of selecting the next hop until the packet reaches the sink.

During our evaluation, three metrics are used to evaluate the performance of the proposed schemes: remaining energy, latency, and privacy. Remaining energy is defined as the remaining energy of the sensor network. Latency is the time for an event message traveling from the source to the base station. Privacy is the important information for different schemes.

7.2. Simulation Results. According to (6) and (7), Figure 3 shows the total energy expended in the system as a transmission distance increases from 1 m to 10 m and the energy expended in the total transmission hops increases from 1 to 1600, for the scenario where each node has a 4096-bit data packet to send to the base station. This shows that when the transmission energy is the same as the received energy from Table 1, a short transmission distance or the few transmission hops can decrease the energy of the whole sensor network.

In Figures 4 and 5, we calculate the average remaining energy of nodes with different algorithms. And higher

Table 2: Simulation parameters table.

Symbol	Definition	Values
N	Number of sensor nodes	600–1600
$E_{\text{Tx-elec}}$	Transmitter electronics	50 nJ/bit
$E_{\text{Rx-elec}}$	Receiver electronics	50 nJ/bit
ε_{amp}	Transmit amplifier	100 pJ/bit/m^2
R	Transmission range	10 m
E_I	Initial energy of sensor nodes	10 J
α	Relative influence of pheromone values $\tau(i, j)$	1
β	Relative influence of heuristic values $\eta(i, j)$	5
ρ	Pheromone evaporation	0.3
q_0	The random parameter	0.5
$\tau_{\min}$	The minimum pheromone	0.4
$\tau_{\max}$	The maximum pheromone	0.9
P_{size}	Packet size	512 B

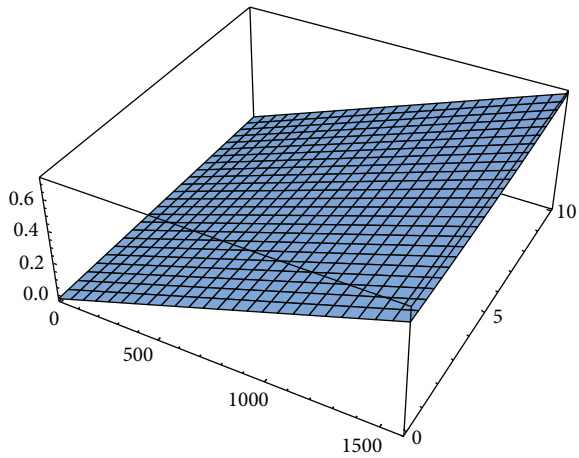

Figure 3: Energy consumption under EELP route scheme (3D).

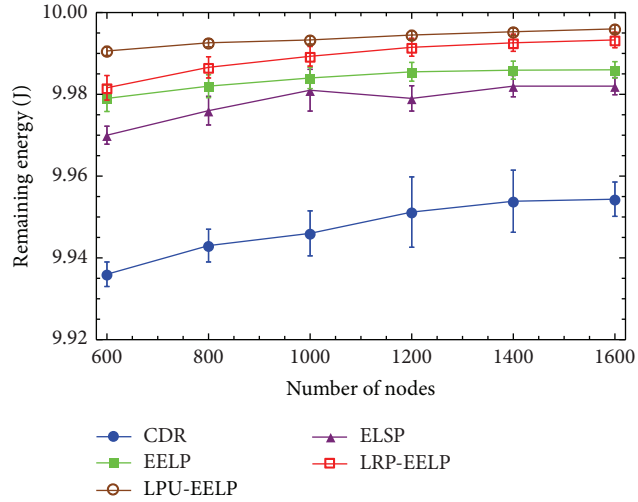

Figure 4: The remaining energy after transmitting 5000 packets.

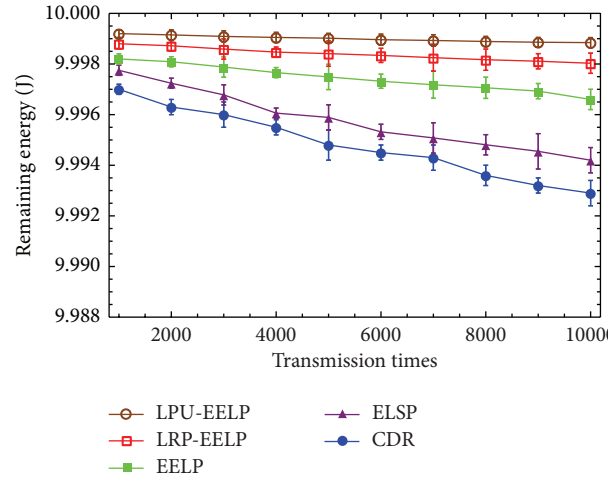

Figure 5: The remaining energy of the network.

remaining energy means less energy consumption. Each algorithm will initialize the topology of the network. With the transmissions going on, some of the algorithms will reconstruct or maintain the topology to balance the energy cost of each node [36]. Hence, the topologies of some algorithms are dynamical.

We can see that the energy consumptions of construction and maintenance of the network topology are high in CDR and ELSP. For CDR scheme, in order to conduct dummy traffic to hide real events, CDR divides the network into several rings according to the hop counts from the sensors to the sink. In each period, the ring where the object appears must establish cyclic diversionary route. And other rings are scheduled to establish cyclic diversionary route with a certain probability p_i. And in a ring, the packet will take a round trip and gather data of all the cluster heads in the ring. So a large number of energies are wasted to establish cyclic diversionary route and transmit dummy packets. Therefore, the CDR scheme costs more energy than others. In ELSP, sensors are divided into different groups. And a proxy node receives transmission packets from other groups and transmits the packets to the key node. Therefore, the proxy nodes and the key nodes will suffer from more energy consumptions than other nodes. Meanwhile, the packets are transmitted through each group in the network, which can generate a heavy burden of all the nodes in ELSP.

In the family of EELP, there is no energy consumption in maintaining or reconstructing the topology; therefore, the average energy cost is lower than other algorithms. The energy consumption concentrates on sending packets to the next hop. After certain rounds of transmissions, the pheromones adjustment will be carried out, which does not cost much energy. From Figures 4 and 5, the relationship among the EELP family in terms of average energy cost is LPU-EELP < LRP-EELP < EELP. So our methods can efficiently save the energy.

From Figures 6 and 7, we calculate energy difference to evaluate the balanced consumption of energy. We aim at

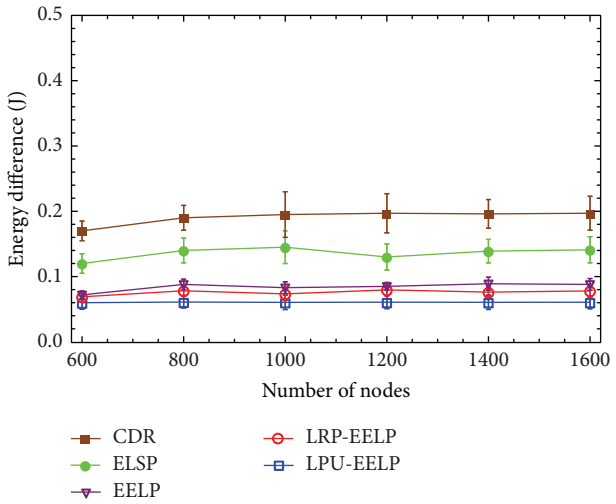

Figure 6: Energy difference after transmitting 5000 packets.

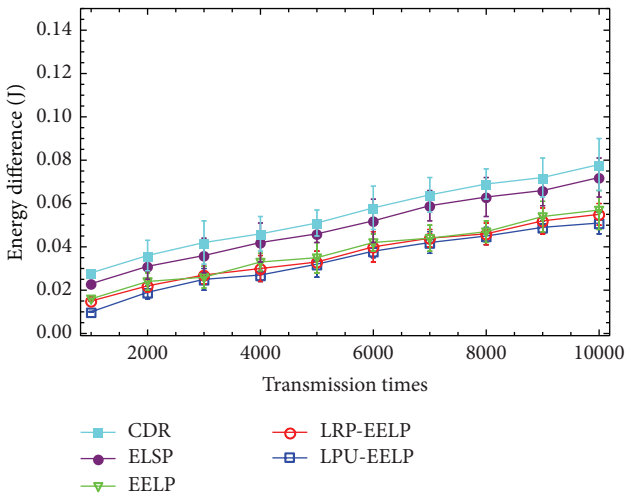

Figure 7: Energy difference of the network.

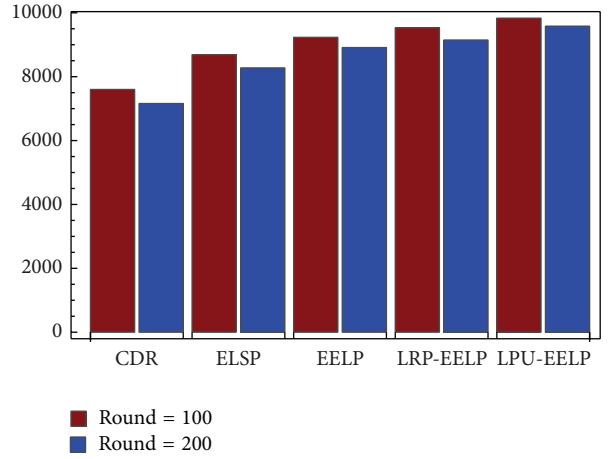

Figure 8: Network lifetime of different protocols.

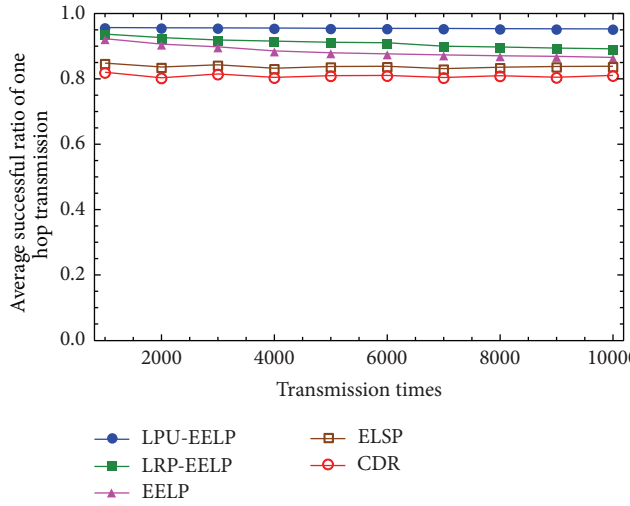

Figure 9: Average successful ratio of one hop transmission.

testifying which method can balance the usage of energy. The balanced consumption can directly affect the lifetime of the network, which is the most prominent feature in energy efficiency in wireless sensor networks. If the energy difference is big, the energy is not averagely used, whereas smaller energy difference indicates the balanced energy consumption.

We can see that the energy difference of CDR is the highest. The reason is that it will establish cyclic diversionary route at different levels with a variant probability. And some nodes send dummy packets to their cluster heads with a probability q. And in a ring, the packet will take a round trip and gather data of all the cluster heads in the ring. So the cluster nodes and its neighbors generate unbalanced energy consumption. Therefore, a big energy difference occurs.

In ELSP, the proxy nodes and the key nodes consume most of the energy. Because the proxy nodes receive the other group packets and send the packets to the key nodes. Then the key nodes transmit the packets to other normal nodes. So the packets must be transmitted by the proxy nodes and the key nodes in a group. Thereby, there is a large energy difference between the proxy nodes or the key nodes and others.

In EELP, when selecting the next hop, each node will estimate the remaining energy of its neighbor to achieve balanced usage of energy. Moreover, in the process of depositing pheromones, the path with minimum energy cost will obtain additional pheromones, by which the balanced usage of energy is implemented. The energy difference relationship among EELP family is LPU-EELP < LRP-EELP < EELP.

The initial energy of each node is set as 0.05 J. We measure how many rounds the network will sustain until any node exhausts in each algorithm. The parameter *updateRound* is set as 100 and 200, respectively. From Figure 8, the EELP family shows longer lifetime than the other algorithms. In CDR, the energies of the cluster nodes will firstly be exhausted because of frequent receiving and transmitting packets. The lifetime of ELSP is short, which the proxy nodes and the key nodes exhaust a lot of energy.

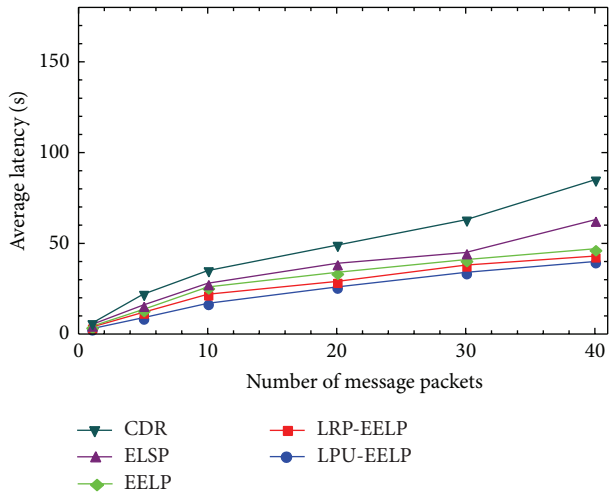

Figure 10: Latency comparison among different routing protocols.

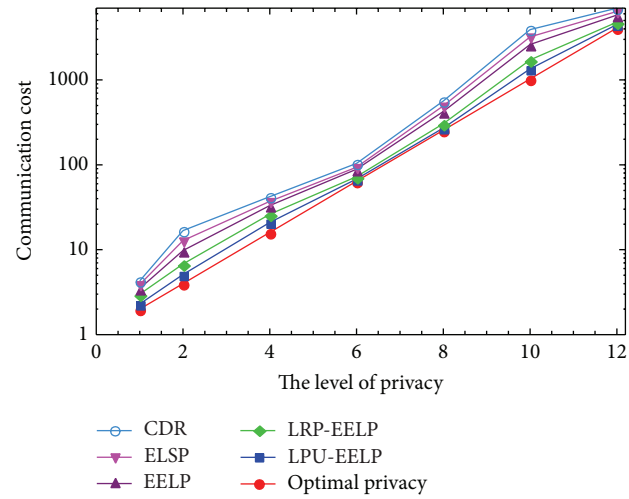

Figure 11: The relationship between communication cost and the level of privacy.

In Figure 9, we analyze the average success ratio of one hop transmission of each algorithm. Packets are sent from the sources to the destination nodes. We count the success ratio of one hop transmission of each packet and calculate the average successful ratio of the one hop transmission. And the successful ratio of EELP is higher than other algorithms.

Figure 10 compares the network transmission latency in different algorithms. In CDR, the packet will take a round trip and gather data of all the cluster heads in the ring. Before the packet is transmitted to the sink, the packet will take a round trip in each ring. And the packet will need time to process the dummy messages in CDR. So the transmission latency will keep rising as the number of rings grows between the source and the sink. In ELSP, the packet will be transmitted to each group. In a group the packet will randomly be sent to the internal nodes. So the transmission latency increases. In EELP family, each node will estimate the remaining energy of its neighbor to send the packets to the next hop. And our methods can choose the short transmission path using the ant colony optimization. So the transmission latency is short in EELP family. The transmission latency relationship among EELP family is LPU-EELP < LRP-EELP < EELP.

Figure 11 shows that we have to pay communication costs to achieve a given level of location privacy. During the simulation, we assume that there is only one object in the network. And whenever a sensor node receives a packet, it will forward it to the next hop as soon as possible. And the object frequently generates the event messages. So the interval is very small. We can see that the communication cost increases as the level of privacy increases. And the communication cost of our method is very close to the performance of the optimal privacy, which is analyzed in Theorem 1. In CDR, cyclic diversionary route and some dummy messages are created to confuse the adversaries. But this can generate massive and unbalanced energy consumption. In ELSP, the packets are transmitted from one group to another group. And the proxy nodes and the key nodes frequently send packets in a group. Although it can protect the source node, it generates more communication cost in ELSP. In EELP family, according to the remaining energy of the neighbor, a node randomly chooses the high remaining energy node as the next hop node. So the EELP family can effectively and efficiently preserve location privacy with practical tradeoffs between communication cost, privacy, and latency.

7.3. Other Characteristic

7.3.1. Robustness. When selecting the next hop, each node will refer to the probability recorded in the routing table, all the paths are dynamical, if a node is removed from the network, only the nodes nearby are required to update the routing table. Therefore, the adjustment of removing a node can be locally achieved. As a result, EELP family owns the feature of robustness.

7.3.2. Fault Tolerance. Suppose errors occur in the element of the node which prohibits it from working. In this case, the node nearby can remove this node from the routing table. Therefore, the faulty nodes will no longer exist in the topology of the network. They cannot affect the transmission of the network. So EELP family is fault tolerant to faulty nodes.

7.3.3. Scalability. Since nodes are deployed randomly in the network, each node only needs to maintain the routing table for dynamically selecting the next hop. Therefore, if a node is added in the network, it only needs to broadcast its identity information and sets up routing table; the nodes nearby are only required to add a new item of the routing table. So we can conclude that EELP family is scalable.

8. Conclusion

In this paper, we focus on the location privacy problem in sensor network. We propose an energy efficient source location privacy protecting scheme (EELP), which applies

the ant colony optimization method to prevent an adversary from back tracing message routing paths to the event source. Whenever a node receives a packet, it will figure out the next hop based on the information of the pheromones, the distance, and the remaining energy according to the routing table. Then each node will update the information. After certain rounds of transmissions, procedure of evaporating and depositing pheromones will be applied which help EELP to adjust the amount of the pheromones. And it can efficiently protect the location information of source node and prolong the network lifetime.

Wireless sensor network is widely deployed to collect valuable information. However, it is obvious that preserving private location information is a big challenge in sensor network. And an eavesdropper may be able to find location information by monitoring and analyzing message routing paths, which can be a serious privacy issue. Our future work is to further study wireless sensor networks and efficiently protect location privacy. And we are extending the proposed protocol to support other functions, such as range query, top k-query, and data aggregation.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by NSFC (Grant nos. 61300181, 61272057, 61202434, 61170270, 61100203, and 61121061) and the Fundamental Research Funds for the Central Universities (Grant nos. 2012RC0612 and 2011YB01).

References

[1] X. Yong, L. Schwiebert, and S. Weisong, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS '06)*, p. 8, 2006.

[2] R. Rios and J. Lopez, "Analysis of location privacy solutions in wireless sensor networks," *IET Communications*, vol. 5, no. 11, pp. 2518–2532, 2011.

[3] S. Pai, S. Bermudez, S. B. Wicker et al., "Transactional confidentiality in sensor networks," *IEEE Security and Privacy*, vol. 6, no. 4, pp. 28–35, 2008.

[4] T. S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno, "Devices that tell on you: privacy trends in consumer ubiquitous computing," in *Proceedings of the 16th USENIX Security Symposium on USENIX Security Symposium (SS '07)*, 2007.

[5] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proceedings of the 10th International Conference on Ubiquitous Computing (UbiComp '08)*, pp. 202–211, September 2008.

[6] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pp. 599–608, June 2005.

[7] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 243–254, August 2000.

[8] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: anonymous on-demand routing in mobile Ad Hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, 2006.

[9] X. Fu, Y. Zhu, B. Graham, R. Bettati, and W. Zhao, "On flow marking attacks in wireless anonymous communication networks," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pp. 493–503, June 2005.

[10] S. Okdem and D. Karaboga, "Routing in wireless sensor networks using an Ant Colony optimization (ACO) router chip," *Sensors*, vol. 9, no. 2, pp. 909–921, 2009.

[11] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.

[12] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-layer enhanced source location privacy in sensor networks," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, pp. 1–9, June 2009.

[13] Z. Ruan, W. Liang, D. Sun, H. Luo, and F. Cheng, "An efficient and lightweight source privacy protecting scheme for sensor networks using group knowledge," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 601462, 14 pages, 2013.

[14] J. Ren, Y. Zhang, and K. Liu, "An energy-efficient cyclic diversionary routing strategy against global eavesdroppers in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 834245, 15 pages, 2013.

[15] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Computer Networks*, vol. 53, no. 9, pp. 1512–1529, 2009.

[16] N. Li, M. Raj, D. Liu, M. Wright, and S. K. Das, "Using data mules to preserve source location privacy in wireless sensor networks," in *Proceedings of the 13th International Conference on Distributed Computing and Networking (ICDCN '12)*, vol. 7129 of *Lecture Notes in Computer Science*, p. 309, 324, Hong Kong, China, 2012.

[17] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An efficient privacy-preserving scheme against traffic analysis attacks in network coding," in *Proceedings of the 28th Conference on Computer Communications (IEEE INFOCOM '09)*, pp. 2213–2221, April 2009.

[18] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP2: timed efficient source privacy preservation scheme for wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '10)*, May 2010.

[19] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.

[20] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical framework for source anonymity in sensor networks," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, December 2010.

[21] K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, "Maximizing lifetime of event-unobservable wireless sensor networks," *Computer Standards and Interfaces*, vol. 33, no. 4, pp. 401–410, 2011.

[22] X. Hong, P. Wang, J. Kong, Q. Zheng, and J. Liu, "Effective probabilistic approach protecting sensor traffics," in *Proceedings*

of the Military Communications Conference (MILCOM '05), vol. 1, pp. 169–175, October 2005.

[23] Z. Zhou and K. C. Yow, "Anonymizing geographic Ad Hoc routing for preserving location privacy," *International Journal of Network Security*, vol. 2, no. 3, pp. 210–218, 2006.

[24] C. Lin, G. Wu, F. Xia, M. Li, L. Yao, and Z. Pei, "Energy efficient ant colony algorithms for data aggregation in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 78, no. 6, pp. 1686–1702, 2012.

[25] T. Camilo, C. Carreto, J. S. Silva, and F. Boavida, "An energy-efficient ant-based routing algorithm for wireless sensor networks," *Ant Colony Optimization and Swarm Intelligence*, vol. 4150, pp. 49–59, 2006.

[26] M. Dorigo, *Optimization, learning and natural algorithms [Ph.D. thesis]*, Dipartimento di Elettronica, Politecnico di Milano, Milan, Italy, 1992.

[27] K. Kalpakis, K. Dasgupta, and P. Namjosh, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks," *Computer Networks*, vol. 42, no. 6, pp. 697–716, 2003.

[28] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '33)*, pp. 1–10, January 2000.

[29] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-layer enhanced source location privacy in sensor networks," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, pp. 324–332, June 2009.

[30] C.-T. Li and M.-S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks," *Information Sciences*, vol. 181, no. 23, pp. 5333–5347, 2011.

[31] N. T. T. Huyen, M. Jo, T.-D. Nguyen, and E.-N. Huh, "A beneficial analysis of deployment knowledge for key distribution in wireless sensor networks," *Security and Communication Networks*, vol. 5, no. 5, pp. 485–495, 2012.

[32] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 406254, 14 pages, 2012.

[33] M. Dorigo and L. M. Gambardella, "Ant colony system: a cooperative learning approach to the traveling salesman problem," *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 53–66, 1997.

[34] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.

[35] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: accurate and scalable simulation of entire TinyOS applications," in *Proceedings of the1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 126–137, November 2003.

[36] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 70–84, July 2001.