Research Article

An Energy-Efficient Cyclic Diversionary Routing Strategy against Global Eavesdroppers in Wireless Sensor Networks

Ju Ren, Yaoxue Zhang, and Kang Liu

School of Information Science and Engineering, Central South University, Changsha 410083, China

Correspondence should be addressed to Ju Ren; ren_ju@csu.edu.cn

Received 29 December 2012; Accepted 13 March 2013

Academic Editor: Mianxiong Dong

Copyright © 2013 Ju Ren et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

While many protocols for sensor network security provide confidentiality for message content, contextual information usually remains exposed, which can be critical to the mission of the sensor network. In this paper, we propose an energy-efficient cyclic diversionary routing (CDR) scheme against global eavesdroppers for preserving location privacy and maximizing lifetime of wireless sensor networks (WSNs). To ensure no impact on lifetime of WSNs, we minimize the energy consumption of hotspots and generate abundant diversionary routing paths in areas far from sink. To enhance the location privacy preservation, we theoretically figure out the probability of the cyclic interference routings in different areas of the network and statistically achieve an energy consumption balance in the entire network. Analysis and simulation results show that CDR significantly improves the security in source-location privacy preservation without reducing the network lifetime.

1. Introduction

A wireless sensor network consists of numerous cheap, small, and resource-constrained sensors that are self-organized to monitor and study the physical world. It bears a promising future in lots of important applications such as environment monitoring, military surveillance, and target tracking. Sensors collaborate to gather data and disseminate the data to sink [1, 2]. However, sensor networks are facing many security threats such as node compromising, routing disrupting, and false data injecting.

Among all these menaces, source-location privacy is of great interest since it cannot be addressed by classical security mechanisms, such as encryption and authentication. Take an example of event reporting in a sensor network. When a sensor detects an event, it transmits a message with event-related information to the sink. Simultaneously, the location of source sensor reveals itself to the adversary, who may be passively eavesdropping the traffic of the network, no matter how strong the data encryption key is [3–5]. The amount of communication overhead to be carried for preserving source-location privacy against eavesdroppers depends on what capabilities adversaries have. The possibility of the existence of a global eavesdropper who can monitor the entire network traffic leads to a great challenge for resource-constrained WSN. A high-assurance solution that can cope with such a powerful attacker adopts a periodic collection method where each sensor periodically transmits encrypted messages regardless of whether there is real data to send or not [5]. In general, periodic transmission together with encryption can effectively conceal the source of real packets from adversaries who do not have the decryption key. However, energy resource is relatively limited and redundant traffic contributes a great deal of energy consumption in WSNs. Thus, it is necessary to develop energy-efficient protocols to mitigate the overhead in periodic collection scheme. A feasible solution is that all sensors periodically generate packets but part of sensors played as proxies to filter dummy traffic.

Several similar methods have been proposed in the past, but the feasibility and the influence on network lifetime have yet to be explored. Since dummy traffic is supposed to be conducted in the entire network to confuse the global eavesdroppers, it definitely results in an explosion of the network traffic. If there are \( n \) sensors simulating the behavior of each source, the network lifetime will drop to \( 1/n \) of the original lifetime. Even with a dummy message filtering scheme, the traffic of the hotspots unavoidably expands to \( d \)
times, where \( d \) is the degree of the sink. In most of sensor networks, the value of \( d \) can usually run up to 5 or even more than 10. Such a formidable traffic expansion of the hotspots also means a sharp decrease in the network lifetime, let alone the traffic expansions in early schemes, in which every sensor of the network generates a fake message and sends it to the sink. Therefore, it is extremely necessary to design an efficient strategy combined with high security and maximal lifetime to improve the disappointing performance in network lifetime of the current techniques.

In this paper, we propose an efficient cyclic diversionary routing (CDR) scheme based on cluster structure to defend against global eavesdroppers in preserving location privacy and to maximize lifetime in wireless sensor networks. CDR is better than the existing studies in that CDR creates more fake sources to confuse adversaries than the traditional schemes, which greatly improves location privacy. At the same time, the network lifetime will not decrease even with an increase of diversionary routes compared with the traditional schemes. The major contributions of this paper can be summarized as follows.

(1) To the best of our knowledge, it is the first time that a source-location privacy preservation strategy has been proposed to defend against global eavesdroppers without sacrificing the lifetime of wireless sensor networks. Because network lifetime depends on the energy consumption of the hotspot and has no direct relationship to the whole network energy consumption, we can allow only real data flow to cross the hotspots and build cyclic diversionary routing paths in areas where the sensors have enough abundant energy to support them [6–9]. Furthermore, we analyze the energy consumption of different ring areas of the network based on our system model and figure out the probability of interference routing path in each ring. Therefore, the security of source-location privacy would be enhanced significantly, and meanwhile the network lifetime would be hardly affected despite the diversionary routing paths.

(2) In applications of the CDR protocol, we can achieve a significant enhancement in network security without reducing the network lifetime. At the same time, it also leads to some network latency in data transmission. Therefore, this protocol is especially suitable for applications that have urgent needs for network security while having moderate needs for network latency. However, in real-time network applications we can still provide trade-offs between location privacy security and data transmission latency.

(3) We conduct extensive simulation under OMNET++ of the proposed scheme CDR. Analysis and simulation results confirm the validity and efficiency of CDR and show that CDR not only significantly improves the security of source-location privacy but also achieves maximal network lifetime.

The rest of this paper is organized as follows. Section 2 reviews the related work. And the system model is described in Section 3. Section 4 presents the details of the CDR scheme. Security analysis and performance analysis are provided in Section 5. Section 6 shows the simulation results and their analysis and comparison. We conclude in Section 7.

2. Related Work

Privacy threats existing in sensor networks can be categorized into two types, namely, (i) content-oriented privacy threats and (ii) contextual privacy threats. The content-oriented privacy mainly concerns the ability of adversaries to crack the content of messages transmitted in sensor networks [1]. While encryption is an effective way to address these problems [10–12], adversaries are still able to extract the contextual information such as source-location from the messages. Therefore, contextual privacy should be studied more carefully due to their importance and urgency.

A number of techniques have been presented to dispose of contextual privacy threats. We can generally divide these works into two groups by the capability of the adversaries: strategies against local eavesdroppers and strategies against global eavesdroppers.

The local eavesdroppers have limited coverage, comparable to that of sensors. At any given time they can thus only monitor a local area. These attackers start from the sink and try to locate source node hop-by-hop in a tracing back way. Several methods have been proposed to address the source-location privacy problem against local eavesdroppers, for example, [4, 5, 13–15]. Kamat et al. proposed a classic and effective phantom routing scheme to solve this problem [13], which can be described as two phases. First, a message is sent through some neighbor sensors to a phantom node which is a random walk away. Then, the message will be either broadcasted or sent in the shortest path to the sink from the phantom node. Since each message probably traverses a different random walk path before being transmitted with greed routing, attackers are supposed to be confused by the diverse phantom source-location, and then the true source will be concealed.

However, the phantom nodes are usually extremely close to the real source, bringing a hidden danger in source-location preservation. Several advanced techniques have been proposed to improve the phantom routing strategy. In [16], researchers proposed a direct walk in section-based or hop-based approach to keep the phantom node away from the real source as far as possible. Li and Ren [4] developed three two-phase dynamic routing strategies to preserve source-location privacy. The main idea is to randomly transmit the message to a sensor far away from the actual source at first and then send the message to the sink with single path routing.

The strategies mentioned above all have outstanding performances in location privacy preservation against local eavesdroppers. However, global eavesdroppers are much more powerful and formidable adversaries compared with the local ones. For their ability of eavesdropping the entire network and traffic analysis, we have to devise more suitable and available schemes to defend source-location privacy against them. Part of related works is listed as follows.

Mehta et al. [17] first presented the global eavesdropper model. They formalized the source-location privacy issue under this strong adversary model and figured out the communication overhead needed for obtaining a given privacy. To address this problem, they proposed two strategies to preserve the location privacy: periodic collection and source
simulation. The periodic collection method provides a high level of location privacy by making each sensor generate dummy traffic periodically. To reduce the enormous energy consumption caused by periodic collection, source simulation method randomly selects several sensors at multiple places to simulate the behavior of real objects to confuse the adversaries. However, fake sources also bring much extra energy consumption to the hotspots of the network, which leads to a poor network lifetime.

Shortly after that, several techniques have been presented to improve the network lifetime based on the idea of source simulation. Proxy filtering is one of the improved strategies. Yang et al. [18] illustrated the main idea of this scheme in a way that they select some sensors as proxies that proactively filter dummy messages on their way to the sink. Then, they proposed two methods named PFS and TFS to accurately locate proxies. Because the problem of optimal proxy placement is NP-hard, they employed local search heuristics with no guaranteed maximal network lifetime.

Recently, Bicakci et al. [19, 20] studied the lifetime in various proxy assignment schemes and different deployment scenarios. They propose a filtering method called OFS (Optimal Filtering Scheme) to maximize network lifetime and preserve source-location privacy against global eavesdroppers. This scheme is based on a Linear Programming framework. They claimed that Linear Programming is an effective method to find the optimal locations of proxies under a set of linear constraints.

Most of the techniques mentioned above can well preserve the location privacy against global eavesdroppers, but fixing the optimal proxy locations is not an easy task, and the network lifetime will be reduced more or less for the intrinsic disadvantage of the locating method. To address this problem, our CDR scheme adopts cluster structures to construct cyclic interference routing paths, in which the cluster heads will act as proxies to filter the fake messages generated by the fake sources. Additionally, we also theoretically figure out the probability of the cyclic interference routing paths in different areas of the network to provide optimal privacy protection without deteriorating the network lifetime.

3. System Model and Problem Statement

3.1. Network Model. We make the following assumptions about our network model.

(1) The wireless sensor network consists of sensor nodes that are uniformly and randomly deployed in a sensor field with density \( \rho \), and they cannot move after being deployed. The sink is located at the center of the network and works as the network controller to collect event data.

(2) We assume the object is equipped with a GPS so that the sink can always be aware of its location. And the appearance of the object is randomly distributed in the entire network, so the probability that each sensor detects the information of the object is equivalent. We also assume that adversaries cannot attack the object within the area that is one hop away around the sink for the powerful monitoring ability in this area.

(3) The sensor nodes are assumed to know their relative locations and the sink location. That is, each sensor node has the knowledge of its neighbor nodes [21]. We also assume that a security infrastructure, such as powerful encryption, has already been built in; that is, no information carried in the message (e.g., packet head) will be disclosed. The key management, including key generation, key distribution, and key update, is beyond the scope of this paper.

3.2. Adversary Model. The adversaries are assumed to be external, passive, and global attackers. By external we mean that the adversaries will not compromise or control any sensors; by passive we assume that the attackers do not conduct any active attacks such as traffic injection, channel jamming, or denial of service attack; by global we presume that the adversaries can collect and analyze all the communications in the network. Note that it does not necessarily mean such global attackers are capable of detecting all the occurrence of real events in any place of the network by themselves, because (i) real event detection devices are often costly, whereas message collection devices are inexpensive and off the shelf; (ii) real event detection devices such as animal-monitoring cameras normally do not have sizes as small as regular sensors which means they are easy to be found and destroyed.

To be more specific, the adversaries may launch the following attacks in our model. On the one hand, even with encryptions of the messages in the network, it is still easy for the adversaries to trace back to the previous source of the messages if the encrypted messages remain the same during their forwarding process. On the other hand, the adversaries may perform more advanced traffic analysis including rate monitoring and time correlation. In a rate monitoring attack, the adversaries pay more attention to the nodes with different (especially higher) transmission rates. In a time correlation attack, the adversaries may observe the correlation in transmission time between a node and its neighbor, attempting to deduce a forwarding path.

3.3. Energy Consumption Model. Sensors consume energy when they are sensing the environment and receiving or transmitting data. The amount of energy consumed for sensing is not related to routing. Therefore, we consider only the energy consumption in transmitting and receiving messages. According to the radio model used in [6], energy consumption for transmitting is given by

\[
E_{\text{tx}} = \begin{cases} 
|E_{\text{elec}}| + 4|E_{\text{amp}}|d^4 & \text{if } d < d_0, \\
|E_{\text{elec}}| + |E_{\text{fss}}|d^2 & \text{if } d > d_0,
\end{cases}
\]

where \( E_{\text{elec}} \) is the transmitting circuit loss. Both the free space \( (d^2 \text{ power loss}) \) and the multipath fading \( (d^4 \text{ power loss}) \) channel models are considered in the model, depending on the distance between transmitter and receiver. \( E_{\text{fss}} \) and \( E_{\text{amp}} \) are the energy required by power amplification in these two
models, respectively. The energy spent in receiving a 1-bit packet is

\[ E_r = IE_{elec} \]  \hspace{1cm} (2)

The above parameter settings are given in Table 1 [5].

For a better understanding of this paper, we detail the meanings of related notations in Table 2.

3.4. Problem Statement. It is a very challenging task to provide source-location privacy under the global adversary model. To prevent the traffic analysis attacks, trade-offs between various performance and security metrics such as privacy, latency, and network lifetime widely exist. If all the packets in the network are real event packets and every node reports, receives, or forwards a real event message immediately, it would be quite easy for a global attacker to trace back to the real source without any delay. Therefore, diversionary routing paths are necessary in the sensor network. But apparently, diversionary routing paths will significantly increase the network traffic, which is undesirable for sensor networks where communication overhead dominates the entire energy consumption. To guarantee the source-location privacy without reducing the network lifetime, we conclude our goals into the following two aspects.

1. The proposed scheme should be secure enough to defend location privacy against the global adversaries; that is, the adversaries should not be able to get the source-location information by analyzing the traffic pattern in any phase of a data gathering period.

2. The network lifetime should be scarcely affected by the diversionary routing paths. Since the sensors in the network are hard to recharge after deployment, the maximal network lifetime is the foremost goal in most applications. And for the reason that it is hard to minimize the event reporting delay along with diversionary routing paths, the proposed scheme should be best suitable for applications where a certain amount of transmission delay could be tolerated.

4. The Cyclic Diversionary Routing Scheme

In this section, we describe our Cyclic Diversionary Routing (CDR) scheme for location privacy preservation and lifetime maximization in wireless sensor networks. The principles of CDR can be expressed as the following three points. (1) All the cyclic interference routing paths and real routing path are homogeneous that the adversaries cannot distinguish them by their shape or size. And we ensure that a number of sensors simulating the behavior of real sources to confuse the adversaries always exist in the network. Therefore, the security of the network is enhanced in any phase of a gathering period. (2) As network lifetime depends on the energy depletion of the hotspots, the proposed strategy will not lay any kinds of additional burden on the hotspots of the network. And the energy consumption in other areas increased by the diversionary routing paths should also be designed to be no greater than the energy consumption of the hotspots. (3) Making full use of the abundant energy in areas far from sink to generate interference routing paths as many as possible, because the sensors in these areas always remain much energy when the network dies. Based on these three principles, we can then get the maximal network lifetime and improve the security of network in one strategy.

4.1. Overview of the Proposed Scheme. To conduct dummy traffic without reducing the network lifetime in hiding real events, we divide the network into several rings according to the hop counts from the sensors to the sink and establish cyclic diversionary route at different levels with a variant probability, just as shown in Figure 1. The main idea can be described as the following aspects. (i) We first divide the rings in areas other than the hotspot area into uniform clusters and name one of cluster heads in the outmost ring as the promoter. (ii) In each period, the ring where the object appears (called event-ring) must establish cyclic diversionary route, while the hotspot (i.e., the first ring) will never create interference route and will only relay the real messages to the sink. And other rings are scheduled to establish cyclic diversionary route with a certain probability \( p_i \). If the sensors of a ring are notified to create interference routing, they are supposed to send dummy messages to their cluster heads with a probability \( q \). When the cluster head receives all the data in the cluster, it will dump all the dummy data, and only the cluster head that is in a cluster where a real event occurs will keep the real data. (iii) Finally, the promoter will start the data transmission to the sink with one initial dummy data package. 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. After the intercluster communication in this ring, it will be forwarded to the cluster head of the next inner ring. Otherwise, it will be forwarded directly to the cluster head of the inner ring. In this method, data package will be safely forwarded to the sink ring by ring. Pay attention that when the data package comes across with the cluster head where a real object exists, dummy data will be replaced by real data in the data package. Therefore, if a real event occurs, only real data can finally make to the sink.

Specifically, the advantages of CDR mainly lie in the following two aspects.

1. Improvement on security: in order to effectively defend against global eavesdroppers, at any given time dummy events that are homogeneous with real events must exist in the network. And also, the clusters where cluster members send dummy data to their cluster heads are completely the same as the cluster with the real source. In this case, adversaries cannot distinguish the real source from ways of intracluster communication. After intracluster data aggregation, each cyclic diversionary route is generated in the same way. Therefore, adversaries still cannot track back to a specific cyclic diversionary route since intercluster communications are all the same. In general, we provide secure preservation of location privacy at any phase of our strategy.

2. Enhancement on network lifetime: it is well known that there are hotspots near the sink in WSNs, and usually, after the first node dies, the network can no longer perform
complete and effective monitoring of the entire network. Therefore, the network lifetime is usually defined as the last time from the beginning of the network till the time the first node dies [6]. Generally speaking, the security of location privacy is proportional to the amount of dummy traffic. While dummy traffic usually leads to a decrease in network lifetime. As we discussed in the section above, previous research mainly brings in a proxy filter scheme to provide trade-offs between network lifetime and security in which network lifetime can still be affected more or less. In CDR scheme, we adopt cluster heads to filter dummy packets in the cluster structure. In this case, despite the interferencedatageneratedinthewholenetwork,intercluster communication flow will always keep at a moderate level. Moreover, we have no extra energy consumption of the hotspots and energy still remains in those rings even after generating the diversionary route. Theoretically, the CDR scheme can both preserve location privacy and maximize the network lifetime.

4.2. Description of Cyclic Diversionary Routing Scheme. To provide more detailed descriptions of our protocol, we divide the CDR scheme into three phases, (i) initialization and clustering; (ii) intracluster data aggregation; (iii) cyclic diversionary route establishment. In the following text, we will describe the procedures of the proposed cyclic diversionary routing scheme in detail.

(i) Initialization and Clustering. In our network model, we first divide the network into several rings according to the hop counts from the sensors to the sink. We assume that the sink has unlimited resources and works as the network controller to collect event data. Then we divide the rings in areas other than the hotspot area into uniform clusters. The clustering methods have been proposed in [22–25], and here we adopt the HEED clustering algorithm in [18], which can well balance the energy consumption of nodes in the same ring and the size of clusters in the network. Additionally, we select a cluster head in the outmost ring as the starting node of the cyclic diversionary route, which we call the promoter. And the token scheme presented in [26, 27] can be applied
here to randomly select the promoter in the outmost ring who holds the token at first and then passes it to the other cluster heads during clustering process.

At the initial stage of every period, rings other than the event-ring and the first ring are scheduled to establish cyclic diversionary route with a certain probability $p_i$. Based on this probability, the sink can learn about the routing information of different rings and broadcast this information to nodes in the network. And we call those rings assigned to create diversionary route interference rings.

(ii) Intracuster Data Aggregation. With the initial information, the cluster heads in interference rings will start gathering information among their cluster members. In this phase, the real source will send the real data to its cluster head, while other cluster members turn into fake sources with a certain probability $p$ and then send dummy messages to their cluster heads.

Apparently, with more nodes involved in intracluster communication, we bring more confusion to the eavesdroppers, which results in a safer privacy of the network. However, from the energy perspective, more fake sources undoubtedly lead to more energy consumption of the network. In order to provide trade-offs between energy consumption and network security, here we randomly select part of the sensors to generate dummy messages and send the messages to their cluster heads, while cluster heads will then dump all the dummy messages they received and only keep the real message that was sent by a real source node. In this case, real event will be safely covered and real data will be successfully stored in the cluster heads of the interference ring.

(iii) Cyclic Diversionary Route Establishment. After the aggregation of intracluster data, the promoter in the outmost ring will start the data forwarding. At first, it will make a decision whether to generate interference routing or not based on the initial information. If an interference route is scheduled to create in this ring, the promoter will take its right neighbor as the next hop of data transmission, and the neighbor node will forward data from cluster head to cluster head around the whole ring in the same way. During the forwarding process, a cluster head that receives the data will check if it holds the real data or not. If so, it will drop the fake data and send the real data to the next hop, otherwise it will just relay the receiving data. Once the data has arrived at the promoter again, the cyclic diversionary route of this ring has finished. Then the promoter will find the cluster head which is the nearest to the sink in the adjacent inner ring and forward the data. This cluster head is supposed to make a judgement the same as the promoter or its previous node and take appropriate actions. While if no interference route is scheduled to generate in a ring, the promoter or the cluster head will just relay the data to the cluster head nearest to the sink in the adjacent inner ring directly. In this way, the data package will be forwarded to the sink orderly in the end. Figures 2 and 3 show the cyclic routing in a ring without or with a real event, respectively.

Through the above procedures, we can successfully generate interference routings in the whole network in one period to defend against global eavesdroppers. In the next period, we make minor adjustment in this scheme according to the location of the real event. As we know global adversaries have powerful abilities in rate monitoring and time correlation which means they can locate the event-ring by analyzing the frequencies of the interference routing generation in different rings. For example, if the adversaries notice that the xth ring has generated the interference routing in 10 periods in a row, they can basically deduce that the real object has stayed in this ring for a long time. Actually in practical applications, objects all have high probabilities to stop over at one place during a relatively long time. In this case, we introduce adjustment in our scheme to defend against the statistics attack of global eavesdroppers.

Broadcast scheme of the sink in CDR can well resist this kind of attacks. If the object stays in the same ring, we also generate interference routings in the same rings exactly as in last period. The adversaries can no longer perform statistics attack since the data flow in the whole network nearly remains the same. The Pseudocode of CDR algorithm is provided in Algorithm 1.

4.3. Energy Consumption Analysis. According to the above details of the CDR protocol, we see that CDR can effectively confuse the adversaries with the redundant traffic which may also lead to huge extra energy consumption on the whole network. We have to theoretically figure out the probability $p_i$ of a ring to generate interference routing and the probability $q_i$ of a cluster member to send dummy messages in this interference ring. With greater $p_i$ and $q_i$, we will certainly have better network security along with much more dummy traffic. We have to further improve the network security in the precondition that extra energy consumption in the rings will not reduce the network lifetime.

Along with the three procedures of CDR establishment described above, the network energy consumption in CDR also mainly consists of three parts: clustering, intracluster data aggregation, and cyclic diversionary routing establishment. In one data aggregation period, cluster members send dummy messages with a certain probability and not too much data flow will send through the cluster head. In this
Cyclic Diversionary Routing

Phase I: Initialization (in sink)

(1) Let $L_p$ denote the ring where the objective exists and $\text{Inter}f_{L_p} \leftarrow 0$, $\text{Inter}f_{L_0} \leftarrow 1$;
(2) For each level $L_i$ of all the levels except $L_0$ and $L_p$ do
(3) Decide the value (0 or 1) of $\text{Inter}f_{L_i}$ with a probability of $p_i$;
(4) End for
(5) Randomly choose a node $N_k$ of the outmost ring to hold the token of promoter, for example $pt = N_k$;
(6) Broadcast the $\text{Inter}$ and $pt$ to all of sensors.

Phase II: Intra-cluster data gathering (in each sensor)

(7) All of sensors except those in the hotspot begin to cluster with HEED clustering algorithm;
(8) After clustering, the node with the token of promoter is supposed to deliver the token to his cluster head.
(9) For each cluster member of each cluster do
(10) Decide to transmit dummy message to his cluster head with a probability of $q$;
(11) End for.

Phase III: Cyclic diversionary route establishing

(12) For each sensor $t$ that stays in each ring $s$ do
(13) $\text{trans} = 0$;
(14) If $t$ is the cluster head with the token of promoter then
(15) If $\text{Inter}f_{L_s} == 1$ then
(16) $t$ transmits his data to his nearest neighbor cluster head which is in the same ring and at the right side of $t$.
(17) Else
(18) $t$ transmits his data to the cluster head which is the nearest to the sink among the cluster heads in the lower ring;
(19) End if
(20) $\text{trans} = 1$;
(21) Else
(22) If $t$ has received data from the upper ring then
(23) If $\text{Inter}f_{L_s} == 1$ then
(24) If $t$ has the real data, then it drops the received data and transmits his real data to the next hop of the same ring; otherwise, it just relays this message to the next hop.
(25) Else
(26) If $t$ has the real data, then it drops the received data and transmit his real data to the lower ring; otherwise, it just relay this message to the lower ring;
(27) End if
(28) $\text{trans} = 1$;
(29) Else if $t$ has received data from the same ring then
(30) If $\text{trans} == 1$ then
(31) $t$ transmits his data to the lower ring;
(32) Else
(33) If $t$ has the real data, then it drops the received data and transmit his real data to the next hop of the same ring; otherwise, it just relay this message to the next hop.
(34) End if
(35) $\text{trans} = 1$;
(36) End if
(37) End if
(38) End for

Algorithm 1: CDR protocol Pseudocode.

The case we can extend the cluster head rotation period a little longer and it will not consume much energy in clustering in one data period. Moreover, according to our clustering algorithm, each node has the same probability to be a cluster head. Then statistically, all the nodes consume the same amount of energy in clustering after certain data periods. As a matter of fact, we can define the energy consumption in clustering as a small and fixed number in each period. Thus the energy consumption in intracluster data aggregation and cyclic diversionary routing establishment will be the primary factor affecting network lifetime. We will discuss the nodal energy consumption in the different rings of the network in the following theorems.

**Theorem 1.** Assuming the nodal energy consumption in clustering is $E_c$, then, for the nodes in the $i$th ring of the network,
the average nodal energy consumption in each period $E_{i}^{\text{avg}}$ can be calculated as

$$E_{i}^{\text{avg}} = \begin{cases} \frac{E_{i}^{\sigma, r/2} + E_{i}^{r}}{\pi r^2 \rho}, & \text{when } i = 1, \\ E_{c} + \frac{p_{i} q (N_{i} - N_{c}^{i}) (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})}{N_{i}} + \frac{p_{i} N_{i}^{c} (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})}{N_{i}}, & \text{when } i \neq 1, \end{cases}$$

(3)

in which $N_{i}$ and $N_{c}^{i}$ can be represented as the following equations:

$$N_{i} = S_{i} \rho = \pi \rho (2i - 1) r^2,$$

$$N_{c}^{i} = \frac{S_{i}}{S_{c}} = \frac{\pi (2i - 1) r^2}{\pi (r/2)^2} = (8i + 4).$$

(4)

Proof. At first, let us focus on the nodal energy consumption in the first ring where the nodes are nearest to the sink. In each data collection period, only one route is generated in this circular area. The average data transmission distance can be defined as $r/2$. Then the whole energy consumption in this area is $E_{1}^{\text{total}} = E_{i}^{\sigma, r/2} + E_{r}^{\sigma}$, and the average nodal energy consumption is $E_{1}^{\text{avg}} = E_{1}^{\text{total}}/\pi r^2 \rho = (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})/\pi r^2 \rho$.

As for the energy consumption in other rings, we can figure it out in combination of two parts.

(1) Energy consumption in intracluster communication: the whole network has been divided into several circular rings with the same width $r$ and the area of the $i$th ring is $S_{i} = \pi (r/2)^2 - \pi ((i - 1)r)^2 = \pi (2i - 1)r^2$, and the number of nodes in the $i$th ring is $N_{i} = S_{i} \rho = \pi \rho (2i - 1)r^2$. According to clustering strategy we divide the rings into uniform clusters with a radius $r/2$; then the area of each cluster is $S_{c} = \pi (r/2)^2$ and the cluster number in each ring is $N_{c}^{i} = S_{i}/S_{c} = \pi (2i - 1)r^2/\pi (r/2)^2 = (8i + 4)$. If a ring has no schedule to generate interference route, then energy consumption in this part is zero. Otherwise, we can figure out the energy consumption in intracluster data aggregation in the following way. Each cluster member generates a dummy message with a probability $q$ and sends the dummy message to the cluster head, and the data transmission distance is half of the cluster radius. Energy consumption in one cluster is $e_{i}^{\text{in}} = qE_{i}^{\sigma, r/2}$. And the energy consumed by the cluster head when receiving an intracluster data is $E_{i}^{\sigma, r/2}$. Hence, the nodal energy consumption in intracluster communication can be calculated as

$$e_{i}^{\text{in}} = \frac{(N_{i} - N_{c}^{i}) (e_{i}^{\text{in}} + qE_{r}^{\text{in}})}{N_{i}} = \frac{q (\pi \rho (2i - 1) r^2 - (8i + 4))}{\pi \rho (2i - 1) r^2} (E_{i}^{\sigma, r/2} + E_{r}^{\sigma}).$$

(5)

As for the $i$th ring with a probability $p_{i}$ to generate interference route, the average nodal energy consumption in intracluster communication in each data collection period can be calculated as $E_{i}^{\text{avg}} = e_{i}^{\text{in}} p_{i}$.

(2) Energy consumption in cyclic diversionary routing: when the $i$th ring generates the cyclic diversionary routing, every cluster head in this ring will send and receive data for one time. And the data transmission distance can be defined as twice of the cluster radius; then here it is $r$. So the average energy consumption in the $i$th ring with interference route to generate is $e_{i}^{\sigma} = N_{i}^{c} (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})/N_{i} = (8i - 4)(E_{i}^{\sigma, r/2} + E_{r}^{\sigma})/\pi \rho (2i - 1) r^2$. Combining with the probability $p_{i}$, the energy consumption in cyclic diversionary routing of the $i$th ring in one data period is $E_{i}^{\text{avg}} = e_{i}^{\sigma} p_{i}$.

No matter whether the $i$th ring has to generate the interference route or not, one cluster head has to forward data to the cluster head in the inner ring to create the main routing to the sink. The transmission distance can be defined as $r$ and this energy consumption is $E_{i}^{\text{backbone}} = (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})/N_{i} = (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})/\pi \rho (2i - 1) r^2$.

In conclusion, the energy consumption of the $i$th ring ($i \neq 1$) can be calculated as the following formula:

$$E_{i}^{\text{avg}} = E_{c} + E_{i}^{\text{in}} + E_{i}^{\text{backbone}}$$

$$= E_{c} + \frac{p_{i} q (\pi \rho (2i - 1) r^2 - (8i - 4)) (E_{i}^{\sigma, r/2} + E_{r}^{\sigma})}{\pi \rho (2i - 1) r^2} + \frac{p_{i} (8i - 4)(E_{i}^{\sigma, r/2} + E_{r}^{\sigma})}{\pi \rho (2i - 1) r^2} + \frac{E_{i}^{\sigma, r/2} + E_{r}^{\sigma}}{\pi \rho (2i - 1) r^2}.$$
Then, to further improve the source-location privacy security, we must keep a balance between the average nodal energy consumption $E_i^\text{avg}$ of nodes in each ring. Thus, we have $E_i^\text{avg} = E_{i+1}^\text{avg} \mid i \in \{2, \ldots, m-1\}$, which is

$$p_2q \left( N_2 - N_2^\text{c} \right) \left( E_i^{\sigma/r2} + E_r^\sigma \right) + p_1N_2^\text{c} \left( E_i^{\sigma/r} + E_r^\sigma \right) + E_i^{\sigma/r} + E_r^\sigma$$

$$= \frac{p_3q \left( N_3 - N_3^\text{c} \right) \left( E_i^{\sigma/r2} + E_r^\sigma \right) + p_2N_3^\text{c} \left( E_i^{\sigma/r} + E_r^\sigma \right) + E_i^{\sigma/r} + E_r^\sigma}{N_2}$$

$$= \ldots = \frac{p_mN_m \left( E_i^{\sigma/r} + E_r^\sigma \right) + E_i^{\sigma/r} + E_r^\sigma}{N_m}.$$  (9)

Once we integrate the two above constraints, Theorem 2 can be proved.

**Inference 1.** The network lifetime in this work, where several extra cyclic routes are created, is the same as that of the shortest path routing.

**Proof.** If the energy consumptions of other rings are no greater than the first ring, the network lifetime is determined by the first ring who has the highest level of energy consumption. If the energy consumption of the first ring in these two strategies are the same, then the network lifetime are the same. As we can see from the previous discussion, only one route to the sink is created, and with the strategy in this work, several cyclic diversionary routes are created, but still there is only one route in the first ring. Besides, even with diversionary routes created in other rings, according to Theorems 1 and 2, the energy consumption of other rings will not be greater than the first ring, so the network lifetime of these two strategies remains the same.

5. **Performance Analysis**

In this section, we will analyze the security of the proposed cyclic diversionary routing scheme. Then through network security criteria and lifetime criteria, we figure out the probability $p_i$ to generate interference route in each ring and the probability $q$ of cluster members to send dummy messages in that ring. Finally, we make an evaluation of the transmission delay of the network. To obtain the best security with the assurance of maximal lifetime, we propose the following algorithms to figure out $p_i$ and $q_i$.

5.1. **Security Analysis.** For the powerful detection ability of global eavesdroppers, we must generate several fake events to confuse the adversaries at random time. The numbers of these events can well speak of the network security. Since the adversaries cannot distinguish the real events from all the events that occur in the network, we can achieve a better network security with more homogeneous events at certain time.

**Theorem 3.** In CDR scheme, the security of location privacy against global eavesdroppers has been improved $S_{\text{CDR}}$ times, and $S_{\text{CDR}}$ meets the following equation:

$$S_{\text{CDR}} = \sum_{i=1}^{m} N_i \cdot p_i = \left( \pi pr^2 + 4q \right) \left( m^2 + m - 2 \right)$$

$$+ (m - 1) \left( 4q - \pi pr^2 - 4 \right).$$  (11)

**Proof.** From the establishment process of CDR, we can see only 3 steps involved in data transmission. Since the main routings are generated in every period and all start from the outer ring to the inner ring in the shortest path, adversaries can find nothing useful from the main routings. And also in cyclic diversionary routes, we apply the same rules in generating interference route and all the cyclic diversionary routes are homogeneous.

In this case, all the cluster members that send dummy messages and the cluster heads in rings that generate the interference routes in CDR scheme can effectively confuse the adversaries in source-location analysis. In other words, numbers of all the cluster members that send dummy messages and the cluster heads in those rings can be seen as security enhancement levels in our CDR scheme.

In one data aggregation period, if the $i$th ring generates the interference route, the numbers of cluster members involved in intracluster communication are $N_i^{\text{cf}} = (N_i - N_i^c) \cdot q + N_i^c = \pi r^2(2i - 1)r^2 + (1 - q)(8i - 4)$. Since the $i$th ring has the probability $p_i$ to generate interference route, we can find that in one period CDR scheme can provide $S_{\text{CDR}}$ times the security level than that of the greedy routing which has no network security protections:

$$S_{\text{CDR}} = \sum_{i=1}^{m} N_i \cdot p_i = \left( \pi pr^2 + 4q \right) \left( m^2 + m - 2 \right)$$

$$+ (m - 1) \left( 4q - \pi pr^2 - 4 \right).$$  (11)

5.2. **Parameters in CDR Scheme.** From Theorems 2 and 3, the probabilities $p_i$ and $q$ both affect the network lifetime and network security. Here we meet an NP-hard problem to achieve the optimization of two parameters. To obtain the best security with the assurance of maximal lifetime, we propose the following algorithm to figure out $p_i$ and $q_i$.

5.3. **Delay Analysis.** In this section, we will discuss the delay caused by the CDR scheme in detail. In CDR scheme, we cannot ensure the shortest delay of data transmission since we have much delay in intracluster communication and cyclic diversionary routing. With more interference routes and more cluster members to send dummy messages, we have better network security and also longer transmission delay.
From the first algorithm, we find that transmission delay gets maximum when all the rings generate interference routes other than the first ring, which also brings a maximal network security. Algorithm 2 gives a detailed method to figure out the probability pi. Then we can calculate the average transmission delay in CDR scheme.

**Theorem 4.** Assume the average delay of data transmitted from a sensor to its neighbor sensor is \( d_u \). Then, in CDR scheme, the delay of the real data message from being sent to being received by the sink is

\[
D_{CDR} = \pi \rho \left( \frac{r}{2} \right)^2 d_u + \sum_{i} d_u p_i (8i - 4) + \left\lfloor \frac{R}{r} \right\rfloor d_u. \tag{12}
\]

**Proof.** Here we also divide the transmission delay into three parts.

1. Delay in intracluster communication: according to our clustering algorithm, we use the TDMA method to conduct intracluster data aggregation. Since data package has an average transmission delay \( d_u \) in every hop, we can assign the time slot for each cluster member as \( d_u \). The quantity of nodes in one cluster is \( N_{cn} = \pi (r/2)^2 \cdot \rho \). So our delay in intracluster aggregation is the same as the overall time slots of the cluster members, which is \( D_{in}^u = N_{cn} d_u = \pi \rho (r/2)^2 d_u \).

2. Delay in cyclic diversionary routing: we forward our data around cluster heads hop by hop in a ring that needs to generate interference route with probability \( p_i \). The number of the cluster heads in the \( i \)th ring can be calculated from Theorem 1 as \( N^c_r = 8i - 4 \). So in the \( i \)th ring we have a transmission delay \( D_{cr}^c = N_c d_u = d_u (8i - 4) \). In this case, we can calculate the average delay in cyclic diversionary routing in one data aggregation period as \( D_{c}^a = \sum_{i} D_{cr}^{c} p_i = \sum_{i} d_u p_i (8i - 4) \).

3. Delay in backbone routing: according to our routing protocol, we generate a backbone route in every data aggregation period which starts from the outermost ring to the sink in greedy routing way. The number of rings in the network is \( N_r = \left\lfloor \frac{R}{r} \right\rfloor \), so the delay in backbone routing can be expressed as \( D_{br}^c = N_r d_u = \left\lfloor \frac{R}{r} \right\rfloor d_u \).

After integrating all the information above, we figure out our transmission delay \( D_{CDR} \):

\[
D_{CDR} = D_{in}^u + D_{cr}^c + D_{br}^c = \pi \rho \left( \frac{r}{2} \right)^2 d_u + \sum_{i} d_u p_i (8i - 4) + \left\lfloor \frac{R}{r} \right\rfloor d_u. \tag{13}
\]

### 6. Experimental Results

In this section, we conduct simulations to compare the performance of CDR scheme with TFS [17] and greedy routing scheme (GR, i.e., a scheme without any preservation measure, in which a sensor sends the real message to the sink once detecting an object). The simulation is based on OMNET++, which is an open network simulation platform for large network. In this simulation, sensors are randomly deployed in a circular area and the sink is located at the centre of the field. In the case of unspecified network parameters, \( R = 500 \text{ m} \), \( r = 80 \text{ m} \), \( \rho = 0.002 \), \( \sigma = 1000 \text{ bits} \), and cluster radius is half of the transmission range. Because TFS is more applicable to square networks, we set the TFS network in a \( 2R \times 2R \) square area. To ensure a similar network situation with GR and CDR, \( R, r, \rho \), and \( \sigma \) keep the same values as before. According to the settings in [17], we set the tree level in TFS as two and divide the network into a number of cells. Given the balance consideration of both energy consumption and network security, a cell is randomly selected to generate real event messages and other 20% cells generate fake messages. For a better analysis of the network lifetime and data latency, we assume a period \( P = 10 \text{ h} = 36000 \text{ s} \) in which the network detects the object and sends data to the sink, and the data transmission delay from one node to another is \( d_u = 2 \text{ s} \). And in the TFS scheme, the buffer interval \( T_{proxy} \) is set as \( 5d_u \). Other settings of the network are shown in Table 1.

6.1. Experimental Results of Energy Consumption and Network Lifetime. In Section 4, we made a detailed analysis of the energy consumption in CDR and worked out the energy constraint formula to ensure network security in the context of maximal network lifetime. In this subsection, we evaluate the simulation results of the energy consumption and network lifetime in CDR scheme.

Figure 4 shows the nodal energy consumption in different regions under GR scheme and CDR scheme. We draw this curve with the average data from 1000 times of data gathering. As shown in this figure, we can see that in GR scheme, hotspots near the sink consume much more energy than other nodes, and after the peak in energy consumption, nodes consume lesser energy as they are further away from the sink. Particularly in regions near the boundaries of the network, nodal energy consumption approaches to zero. However, in CDR scheme, nodal energy consumption shows a different trend. Hotspots near the sink still consume much energy and after reaching the peak, the energy consumption curve falls a little. Then with the increase in distance from the sink, nodal energy consumption level gradually rises and is maintained with a slight fluctuation below the peak in the end, which shows that with interference routings and looping strategy, CDR scheme successfully makes full use of the abundant energy in outer areas of the network and enhances the energy efficiency of the network.

Figures 5 and 6, respectively, show the 3D map of energy consumption in GR scheme and CDR scheme.

Figure 7 gives a detailed comparison of total energy consumption of the network between GR scheme and CDR scheme in one data aggregation period. From this figure, we can see that the whole network consumes much more energy in CDR than in GR scheme. We create many fake sources to increase network security with the abundant energy in outer areas of the network and these fake sources still consume more energy when they send fake messages. Figure 8 shows the tendency of different probabilities of interference routing generation in rings in relation to different probabilities of intracluster data aggregation. We can see that \( p \) and \( q \) have a...
(1) \( p_{\text{optimal}}^{i} = 1, q_{\text{optimal}}^{i} = 0, S_{\text{max}} = 0 \)
(2) while \( q < 1 \) do
(3) Figure out the nodal energy consumption of the outmost level \( E_{m}^{\text{avg}} \) with Theorem 1;
(4) According to Theorem 2, we can compute the maximum value of \( p_{m}^{q} \) by the inequality of \( E_{m}^{\text{avg}} \leq E_{1}^{\text{avg}} \) and get the probability of establishing diversionary route in each level \( p_{i}^{q} \) with \( E_{i}^{\text{avg}} = E_{m}^{\text{avg}} \) | \( i \in \{2, \ldots, m\} \).
(5) Work out the enhancement of location privacy security \( S_{q} \) according to Theorem 3;
(6) if \( S_{q} < S_{\text{max}} \) then
  \( p_{\text{optimal}}^{i} = p_{i}^{q} \) | \( i \in \{2, \ldots, m\} \);
  \( q_{\text{optimal}} = q_{i} \);
end if
(7) \( q = q + \varepsilon \), here \( \varepsilon \) is a very small increment;
(8) end while
End

Algorithm 2: Algorithm for figuring out \( p_{i} \) and \( q \) to get the strongest security performance.

Figures 9 and 10 compare the network lifetime of three protocols from different aspects. As shown in Figure 9, network lifetimes in GR and CDR schemes are basically the same with different transmission ranges while network lifetime in TFS is much shorter. We can find the explanation in Theorem 2. Since the network lifetime depends on the energy consumption of hotspots that are in one hop range of the sink, as long as we bring no extra energy consumption to these hotspots and keep the energy consumption of outer areas lower than this hotspot area, we can promise a maximal lifetime. Figure 10 gives the different network lifetimes in GR and CDR scheme with different network radii in different data aggregation rate. With a certain data aggregation rate, network lifetimes in GR and CDR nearly remain the same regardless of the change in network radii. With a certain network radius, network lifetime keeps rising along with the growing data aggregation period both in GR and in CDR schemes.

6.2. Experimental Results of the Security and Delay Performance. In the previous subsection, we analyze the energy consumption and network lifetime in CDR scheme and verify its energy efficiency. In this subsection, we test the security performance and transmission latency of this scheme. In
our network model, the adversaries have a powerful ability in time correlation but cannot distinguish the authenticity of the data. In this case, we assume that all the nodes that perform intracluster communication in one period are the fake sources in the network. And we can treat the number of the fake sources as the criteria in network security evaluation.

Figure 11 compares the network transmission delay in three protocols. In GR scheme, once a real event is detected, the real source will directly forward this message to the sink in every period. And the transmission delay keeps rising as the distance grows between the sink and the event. In TFS scheme, proxies need time to process the fake messages which results in waiting delay and queuing delay. Therefore, transmission delay is a little longer in TFS scheme than in GR scheme. However, in CDR scheme, the transmission delay in one period of data aggregation is much longer than in both of the previous schemes. While with different locations of the real source in any part of the network, transmission delay maintains a minor fluctuation within certain boundaries. From Theorem 4 we can find that intracluster communication and intercluster communication both lead to transmission delay of the network, but the latency will not change much despite the different locations of the real source. Actually this feature can provide source-location privacy against the adversaries’ ability in time correlation which will possibly help to locate the object. Figure 12 gives the relation between
network security and network scale in GR, TFS, and CDR schemes. It can be seen that, in TFS scheme and CDR scheme, more fake sources are created to confuse the adversaries and bring more powerful security, and the security of the CDR scheme is much stronger than the others'. Moreover, as the scale of the network grows, the CDR scheme increasingly enhances the security of the network.

Figures 13 and 14 show the different transmission delays and network security with different transmission ranges in CDR scheme. In Figure 13, transmission delay drops as the transmission rate rises and it reaches the valley around $r = 90$ m. After that, it rebounds to rise as the $r$ keeps rising. While with the same $r$, transmission delay exponentially multiplies as $R$ keeps rising. All these results clearly indicate that network scale directly affects the transmission delay, and we can certainly find the proper $r$ to achieve optimal data latency in a given network. In Figure 14, we can see that the network security drops as $r$ rises and it rises in proportion as $R$ rises with the same $r$. This shows that with smaller $r$, more rings are formed in the network and more interference routings are generated.

7. Conclusion

In this paper, we present an energy-efficient cyclic diversionary routing scheme based on clustering against global eavesdroppers in wireless sensor networks. The proposed scheme makes full use of the remained energy in regions far away from the sink to create cyclic diversionary routes as many as possible while with only one route in the region near the sink. This strategy improves the network security without sacrificing the network lifetime. Furthermore, we
theoretically figure out the probabilities of different rings to generate interference routings and the probabilities that nodes send dummy messages. We find the optimal routing protocol to secure source-location with maximal network lifetime. Extensive performance analysis shows that the CDR scheme is better than the existing privacy preservation protocols.

Given the powerful abilities of the adversaries in network attack, our scheme is of special significance in source-location privacy preservation. While with an enhancement in network security, it also brings some data transmission delay to the network, which causes some influence in real-time applications. Therefore, in our future research, we will focus on the network latency optimization under the preconditions of a certain level of network lifetime and network security.

**Acknowledgments**

The authors are grateful to the anonymous reviewers for their industrious work and insightful comments. This work is supported by Mittal Innovation Project of Central South University under Grant no. 12MX15.

**References**

[1] H. Zhu, X. Lin, R. Lu, P. H. Ho, and X. Shen, “Slab: a secure localized authentication and billing scheme for wireless mesh networks,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3858–3868, 2008.

[2] K. Ota, M. Dong, Z. Cheng, J. Wang, X. Li, and X. S. Shen, “Oracle: mobility control in wireless sensor and actor networks,” *Computer Communications*, vol. 35, no. 9, pp. 1029–1037, 2012.

[3] A. Jhumka, M. Leeke, and S. Shrestha, “On the use of fake sources for source location privacy: trade-offs between energy and privacy,” *Computer Journal*, vol. 54, no. 6, pp. 860–874, 2011.

[4] Y. Li and J. Ren, “Source-location privacy through dynamic routing in wireless sensor networks,” in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM ’04)*, San Diego, Calif, USA, March 2010.

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

[6] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, “A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks,” *IEEE Transactions on Parallel and Distributed Systems*, 2013.

[7] A. Liu, J. Ren, X. Li, Z. Chen, and X. S. Shen, “Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks,” *Computer Networks*, vol. 56, no. 7, pp. 1951–1967, 2012.

[8] A. Liu, X. Jin, G. Cui, and Z. Chen, “Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network,” *Information Sciences*, vol. 230, pp. 197–226, 2013.

[9] A. Liu, Z. Liu, M. Nurudeen, X. Jin, and Z. Chen, “An elaborate chronological and spatial analysis of energy hole for wireless sensor networks,” *Computer Standards & Interfaces*, vol. 35, no. 1, pp. 132–149, 2012.

[10] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[11] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[12] A. Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, “Secure and energy-efficient disjoint multipath routing for WSNs,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 7, pp. 3255–3265.

[13] 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 (ICDCS ’05)*, pp. 599–608, June 2005.

[14] S. Armenia, G. Morabito, and S. Palazzo, “Analysis of location privacy/energy efficiency tradeoffs in wireless sensor networks,” in *Proceedings of the Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet (NETWORKING ’07)*, pp. 215–226, May 2007.

[15] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, “Entrapping adversaries for source protection in sensor networks,” in *Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM ’06)*, pp. 23–32, IEEE Computer Society, Buffalo-Niagara Falls, NY, USA, June 2006.

[16] C. OzTurk, Y. Zhang, and W. Trappe, “Source-location privacy in energy-constrained sensor network routing,” in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’04)*, pp. 88–93, October 2004.

[17] K. Mehta, D. Liu, and M. Wright, “Location privacy in sensor networks against a global eavesdropper,” in *Proceedings of the 15th IEEE International Conference on Network Protocols (ICNP ’07)*, pp. 314–323, Beijing, China, October 2007.

[18] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, “Towards event source unobservability with minimum network traffic in sensor networks,” in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec ’08)*, pp. 77–88, April 2008.

[19] K. Bicakci, I. E. Bagci, and B. Tavli, “Lifetime bounds of wireless sensor networks preserving perfect sink unobservability,” *IEEE Communications Letters*, vol. 15, no. 2, pp. 205–207, 2011.

[20] K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, “Maximizing lifetime of event-unobservable wireless sensor networks,” *Computer Standards and Interfaces*, vol. 35, no. 4, pp. 382–401, 2011.

[21] S. D. Muruganathan, D. C. F. Ma, R. I. Bhasin, and A. O. Fapojuwo, “A centralized energy-efficient routing protocol for wireless sensor networks,” *IEEE Communications Magazine*, vol. 43, no. 3, pp. S8–S13, 2005.

[22] O. Younis and S. Fahmy, “HEED: a hybrid, energy-efficient, and improvement of cost function based energy aware routing algorithm for wireless sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.

[23] V. Mhatre and C. Rosenberg, “Design guidelines for wireless sensor networks: communication, clustering and aggregation,” *Ad Hoc Networks*, vol. 2, no. 1, pp. 45–63, 2004.

[24] Z. Zhou, S. Zhou, S. Cui, and J. H. Cui, “Energy-efficient cooperative communication in a clustered wireless sensor network,” *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3618–3628, 2008.

[25] A. Förster, A. Förster, and A. L. Murphy, “Optimal cluster sizes for wireless sensor networks: an experimental analysis,” *Ad Hoc Networks*, vol. 28, pp. 49–63, 2010.
[26] F. Wei, X. Zhang, H. Xiao, and A. Men, “A modified wireless token ring protocol for wireless sensor network,” in Proceedings of the 2nd IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet’12), pp. 795–799, 2012.

[27] A. Ray and D. De, “Energy efficient cluster head selection in wireless sensor network,” in Proceedings of the IEEE 1st International Conference on Recent Advances in Information Technology (RAIT’12), pp. 306–311, 2012.