Secure and Energy-Efficient Disjoint Multi-Path Routing for WSNs

Anfeng Liu[†‡] , *Member, IEEE,* Zhongming Zheng[‡] , *Student Member, IEEE,*
Chao Zhang[†], *Student Member, IEEE,* Zhigang Chen[†], *Member, IEEE,*
and Xuemin (Sherman) Shen[‡], *Fellow, IEEE*

***Abstract*—Recent advances in micro-electro-mechanical systems (MEMS) technology have boosted the deployment of wireless sensor networks (WSNs). Limited by energy storage capability of sensor nodes, it is crucial to jointly consider security and energy efficiency in data collection of WSNs. Disjoint multi-path routing scheme with secret sharing is widely recognized as one of the effective routing strategies to ensure the safety of information. This kind of scheme transforms each packet into several shares to enhance the security of transmission. However, in many-to-one WSNs, shares have a high probability to traverse through the same link and to be intercepted by adversaries. In this paper, we formulate secret sharing based multi-path routing problem as an optimization problem. Our objective aims at maximizing both network security and lifetime, subject to the energy constraints. To this end, a three-phase disjoint routing scheme, called Security and Energy-efficient Disjoint Route (SEDR), is proposed. Based on secret sharing algorithm, the SEDR scheme dispersively and randomly delivers shares all over the network in the first two phases, and then transmits these shares to the sink node. Both theoretical and simulation results demonstrate that our proposed scheme has significant improvement in network security under both scenarios of single and multiple black holes without reducing the network lifetime.**

***Index Terms*—Keywords: Wireless Sensor Networks, security, network lifetime, black hole, multi-path routing**

I. INTRODUCTION

Wireless sensor networks (WSNs) have been widely deployed for an extensive range of applications, such as intelligent transportation, military and civilian domains [1]–[3]. The characteristics of wireless sensor nodes, such as low cost, simplicity and broadcast, have further accelerated the deployments of WSNs. To this end, advanced wireless techniques, such as vehicular sensor networks (VSN), are emerging to collect sensing data and provide them to users. However, these characteristics may also cause some potential safety risks [4]–[6]. Black hole attack is one of attacks that adversaries may choose to interfere information delivery. In some cases, adversaries may have mobility to increase the number of black holes for achieving a high packet interception probability. Generally, compromised node (CN) and denial of service (DOS) attacks are two kinds of common black hole attack [7], [8]. In CN attack, adversaries try to compromise a subset of nodes to passively intercept the packets traverse through these nodes. In DOS attack, adversaries actively disrupt, change or even paralyze the functionalities of a subset nodes, such that the normal operations of WSNs can not be executed.

Designing routing strategies to bypass black holes is one of effective methods for addressing such kind of security issues. Previous works mainly aim at delivering packets along disjoint multi-path routes, which can be generally summarized as, 1) deterministic disjoint multi-path routing [2], and 2) randomly disjoint multi-path routing [7]. Both routing strategies focus on transmitting copies of packets along the disjoint routes, which are calculated by some multi-path routing algorithms. Randomly disjoint multi-path routing does not have a fixed candidate route for selection. Therefore, it is able to ensure that adversaries can not know the routes even if they obtain the routing algorithms in advance. Some works combine secret sharing and randomly disjoint multi-path routing to further enhance the security of WSNs [7]. However, most previous works do not consider the network lifetime of WSNs, which may lead to a high probability of sensor nodes outage and cause a cessation of normal operations. In this paper, we try to maximize both the network security and lifetime by exploiting an effective randomly disjoint multi-path routing scheme with secret sharing.

The main contributions of this paper are three-fold:

- We formulate the secret sharing based disjoint multi-path routing problem as an optimization problem. Our objective is to deliver sliced packet shares along randomly generated disjoint paths by routing scheme, such that both the network security and lifetime can be maximized.
- By jointly considering the network security and lifetime, we propose a three-phase routing scheme, called Security and Energy-efficient Disjoint Route (SEDR). Firstly, packets are sliced into shares by (T, M)-

[†]School of Information Science and Engineering, Central South University, Changsha, China, 410083.

[‡]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1.

threshold secret sharing algorithm, and our proposed SEDR scheme disperses these shares in a certain region around source node. Secondly, shares are randomly forwarded along identical-hop routes all over the whole network. Finally, the SEDR algorithm transmits shares to sink by using least-hop routing.

- We analyze the security and lifetime performance of WSNs. The packet interception probability of our SEDR scheme is obtained in both single and multiple black holes cases, and the minimal required size of physically secured area is derived. Moreover, our analysis indicates that the network lifetime will not decrease if the radius of network is not less than 4 hops. Extensive simulation results match our theoretical ones, and demonstrate that the SEDR scheme significantly outperforms existing routing schemes in terms of network security and lifetime under a variety of network scenarios.

The remainder of this paper is organized as follows. In Section II, we give a broad review of the existing routing strategies. In Section III, we present the system configurations and problem formulation. Our proposed routing scheme, called SEDR, is introduced in Section IV. In Section V, we analyze the network security and lifetime of SEDR scheme. Simulations results are presented in Section VI. Finally, we conclude our work in Section VII.

II. RELATED WORK

To improve network security for WSNs, multi-path routing strategies [7], [9], [10] have become a hot topic. It can generally be classified into two categories: 1) packets delivery, which directly transmits packets by various paths [10]–[15], and 2) shares delivery, i.e., transforming each packet into shares, then forwarding shares along different routes [16]–[21]. Packets delivery mainly focuses on discovering node-disjoint or edge-disjoint paths for transmission, thus it can enhance the security and robustness of networks. In [10], the Split Multiple Routing (SMR) protocol was proposed to establish two maximally disjoint routes by flooding the ROUTE REQUEST (RREQ) message to the entire network. In [11], the security of sensor network routing protocols was analyzed, and it was found that multi-path routing strategies are one of the effective countermeasure for the selective forwarding attack. In [12], a Multi Dataflow Topologies (MDT) method was designed to counter the selective forwarding attack by dividing the sensor nodes into two-dataflow topologies. However, packets delivery duplicates the transmissions, which may lead to high energy consumption.

Normally, shares delivery uses secret sharing to enhance the security of packet transmission. Based on a secret sharing algorithm [16], the adversary can not decode the packet without intercepting a required number of shares. Therefore, the security performance of the network is improved. Moreover, as there is no need to duplicate packet transmissions, shares delivery can significantly relieve the energy consumption of networks. In [17], based on a distributed N-to-1 multi-path discovery protocol and secret sharing, hybrid multi-path scheme (H-SPREAD) was designed to improve both the security and reliability of wireless sensor networks. In [22], a Secure Message Transmission (SMT) mechanism was proposed to continuously evaluate the performance of each route, then routing of subsequent shares is determined according to the rating of routes. These works focus on deterministic multi-path routing strategies, i.e., the route computation is not changed under the same topology. With random multi-path routing protocols [20], [21], [23], shares delivery can further strengthen and guarantee the security of packet transmission, even if adversaries acquire the routing strategy. In [19], a mathematical framework was presented for analyzing random routing protocols. [7] is the closest past literature to ours. Four propagation schemes were proposed to dispersively deliver the shares of packets, such that the packet interception probability can be guaranteed. However, most previous works do not consider the network lifetime, which is one of the critical issues in WSNs. In our work, we jointly consider both network security and lifetime issues, while aim at designing efficient secret sharing based disjoint multi-path routing scheme to enhance both the security and lifetime performance of WSNs.

III. SYSTEM CONFIGURATIONS AND PROBLEM FORMULATION

We consider a circular region of many-to-one high-density WSNs with sensor nodes uniformly and randomly distributed in it [24], [25]. As wireless sensor nodes are low-cost wireless devices, it is not reasonable to equip sensor nodes with expensive global positioning systems (GPS) devices. Thus, GPS-free sensor nodes are used, while each sensor only needs to have relative location information of itself and its neighbors, i.e. the least number of hops to the sink node. The relative location information is periodically updated between neighbors to ensure the accuracy [26]. When a sensor node detects an event, it will generate messages and send those messages to the sink node [24]. Link-level security based on a conventional cryptography-based bootstrapping algorithm is assumed, which uses symmetric link keys to encrypt consecutive links along each end-to-end path. Thus, we assume that a link key is safe except either side of the link is physically compromised by the adversary [7], [27]. Due to the simplicity of wireless sensor node, WSNs are vulnerable to variety of attacks. Generally, the adversary is able to compromise multiple sensor nodes except the sink and its immediate

surrounding nodes, as these nodes can be easily physically secured by installing video monitoring equipments [7], [22], [28]. Once the sensor nodes are compromised, adversary can form the black holes to acquire all the information of end-to-end paths traverses through these black holes [7]. In order to increase the security, we employ (T, M)-threshold secret sharing mechanism [29], i.e., each packet is broken into M shares and can be decoded only when at least T shares are received.

Our energy consumption model is based on the power consumption model in [24], [30]. The notation is given in TABLE I. According to the distance between the transmitter and the receiver, the energy spent for transmitting ℓ-bit packet over distance d, denoted E_t, can be expressed by free space and multi-path fading channel models as following:

$$E_t = \begin{cases} \ell E_c + \ell \mathcal{E}_{fs} d^2, & d < d_0 \\ \ell E_c + \ell \mathcal{E}_{amp} d^4, & d > d_0, \end{cases} \tag{1}$$

where the energy loss E_c depends on factors such as digital coding and modulation. The energy consumed for receiving this message is $E_r(\ell) = \ell E_c$.

TABLE I
TABLE OF NOTATION

Notation for energy consumption model	
d_0	Distance threshold for different channel models
E_c	Energy losses in transmission circuits
$\mathcal{E}_{fs}$	Power amplification energy in free space model
$\mathcal{E}_{amp}$	Power amplification energy in multi-path fading model

In this paper, we focus on designing routing protocols to maximize the lifetime of WSNs, while guarantee the security of the whole network. Thus, our objective function consists of two parts: maximizing network lifetime and minimizing the probability of eavesdropping. Since the outage of sensor nodes may have significant impacts on network coverage and communications, we denote the network lifetime, Γ, as the period from the starting of network operation until the first power outage occurs in WSNs [24], [31], [32]. Let E_i denote the energy consumption of node i. The objective of maximizing network lifetime can be expressed as

$$\max(\Gamma) = \min \max_{0<i\leq n} E_i. \tag{2}$$

Security level is determined by the probability that black holes can decode the packet, i.e., black holes intercept at least T shares when M shares of an information packet are sent from the source sensor node. Thus, the security is the probability that at least T shares traverse through the black hole in total M shares [7], [29]. Suppose each black hole i occupies a region, namely $\mathcal{N}_i$, and can intercept all the transmitted packets within this region. As black holes may have some overlapping regions, the total area of black holes should be $\mathcal{N} \leq \sum_{n=1}^{k} (\mathcal{N}_i)$. Let ϱ_i stand for the total area that the i-th share T_i can forward the packet. The probability that share T_i is eavesdropped can be expressed as $q_i = \mathcal{N}/\varrho_i$. Since each share has the same probability to be intercepted, we have $q = q_i = q_j$, $i, j \in \{1...M\}$. Therefore, the probability that the adversary can acquire at least T shares is

$$P = \sum_{k=T}^{M} \binom{M}{k} q^k (1-q)^{M-k}. \tag{3}$$

Combining maximizing network lifetime and minimizing the probability of eavesdropping, our objective function can be formulated as follow:

$$\begin{cases} \max(\Gamma) = \min \max\limits_{0<i\leq n} E_i \\ \min(P) | P = \sum\limits_{k=T}^{M} \binom{M}{k} q^k (1-q)^{M-k}. \end{cases} \tag{4}$$

IV. SEDR SCHEME

In this section, we propose Secure and Energy-efficient Disjoint Routing (SEDR) scheme to maximize both the network lifetime and the security. Specifically, SEDR focuses on increasing security by utilizing available energy to forward shares with disjoint routes. We first give an overview of the SEDR scheme in Subsection IV-A, followed by the detailed description in Subsection IV-B. Finally, we introduce the energy consumption analysis in Subsection IV-C.

A. Scheme Overview

As the typical many-to-one traffic pattern leads to uneven energy consumption, the sensor nodes close to the sink node have much higher chances of power outage. When one of the sensor nodes is out of energy in WSNs, the nodes far away from the sink node have used only 10% of their batteries [24], [30]. Thus, our proposed scheme aims at utilizing the redundant energy to dispersively distribute the shares of packets all over the WSNs, and then forward these shares to the sink node along the randomized disjoint routes. The scheme enhances the network security by increasing the diversity of disjoint routes, which significantly decreases the probability of packet interception by adversaries. In the meantime, the least required number of shares M is reduced with the improvement of security, which leads to energy savings.

Our SEDR scheme is composed of three phases: 1) regional dispersive routing, 2) disjoint identical-hop routing, and 3) least-hop routing. Based on the (T, M)-threshold

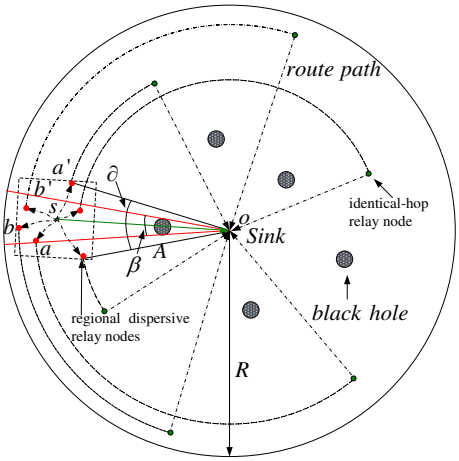

Fig. 1. An example of the SEDR scheme.

secret sharing mechanism, such as the Shamir's algorithm [29], to break the packet into M shares, the M shares are sent to M randomly selected sensor nodes in the regional dispersive routing phase. In disjoint identical-hop routing phase, M shares are transmitted to other sensor nodes dispersively distributed in the network with disjoint routes, where all the sensor nodes along the same routing path have the equal hops to the sink node. Finally, SEDR scheme uses the shortest routing path to forward the M shares to the sink node. An example is shown in Fig. 1. Source node s breaks the packet into 6 shares, and sends them to the randomly selected sensor nodes around the source node, namely regional dispersive relay nodes, then these shares are further forwarded to the sensor nodes randomly selected from the whole network, called identical-hop relay nodes, in disjoint identical-hop routing phase. Finally, M shares are transmitted with shortest routing path to the sink node. Our analysis shows the probability that adversary can decode the packet is close to 0 when there exists one black hole in the WSNs. Even when multiple black holes are in the network, the probability that T shares are intercepted by the adversaries is very low as the area of black hole is tiny comparing with the area of whole WSNs. The redundant energy is utilized to forward the shares of packets along disjoint routes in the whole network, which does not have impact on decreasing the network lifetime. Moreover, with the improvement of network security, the network lifetime is extended as the least required number of shares M is reduced. The details of network security and lifetime analysis are presented in Sec. V.

B. SEDR Scheme

The SEDR scheme tries to increase the diversity of routing paths by forwarding the shares to the sensor nodes dispersively distributed all over the network with disjoint routes. Thus, the regional dispersive routing and disjoint identical-hop routing phases aim at randomly distributing the shares in the whole network, then transmit the shares to the sink node by least-hop routing.

We define the line from the source node to the sink node as X axis and the line orthogonal to X axis at the source node as Y axis. By considering X axis as polar axis, we construct an analogous polar system with the sink node as pole and γ as the hop coordinate, where γ is the hop length from the polar axis along the route consisting of the sensor nodes that have identical hop length to the sink node. The illustration is shown in Fig. 2. Let h denote the hop length from the source node to the sink node, and $-\tau_{max} \sim \tau_{max}$ as the width and height of the region along X axis and Y axis. For regional dispersive phase, we aims at evenly distributing shares in region $[h-\tau_{max}, h+\tau_{max}]$. Initially, each packet is broken into M shares. Each share has a set of information, $(\text{ID}, X_h, Y_h, \gamma_h)$, where ID is used to identify each share. (X_h, Y_h) and γ_h are the randomly generated hop lengths to forward the shares in regional dispersive routing and disjoint identical-hop routing phases, respectively. X_h and Y_h are the hops that the shares should be forwarded along X and Y axis, which are randomly obtained from $\{-\tau_{max}, \tau_{max}\}$. Then, each share is transmitted hop by hop until reaching the determined locations. The hop lengths from the sink node to these shares are randomly distributed in $[h-\tau_{max}, h+\tau_{max}]$. Let γ_h denote the hops of γ that the share should forward from its regional dispersive relay nodes. Similar to regional dispersive routing, each share randomly obtains γ_h from $\{-\gamma_{max}, \gamma_{max}\}$ and is transmitted hop by hop until achieving its identical-hop relay node in disjoint identical-hop routing phase, where γ_{max} is the maximum γ of each share. Finally, the shares are sent to the sink node according to the routes with the least of hop length. The details of SEDR scheme can be found in Algorithm 1.

C. Energy consumption analysis

In the SEDR scheme, we focus on transmitting the shares of packets along the routes distributed in the whole network to enhance the security of the network. Intuitively, the diversity of routes is proportional to the network security. However, the energy consumption of sensor nodes may increase at the same time, which may also lead to a decrease of network lifetime. In order to simplify the analysis of relationship between network security and lifetime, the impact of different parameters, such as energy consumption and distance from the sink to sensors, on network lifetime is illustrated in this subsection.

As the energy consumption of sensor nodes is uneven caused by many-to-one traffic pattern, we analyze the relationship between sensor nodes' energy consumption and locations in each phase. The packet slicing is operated by

Algorithm 1 Secure and Energy-efficient Disjoint Routing scheme

Break packets by (T, M)-threshold secret sharing;
for all Data share s_i **do**
  $X_h \leftarrow Random(-\tau_{max}, \tau_{max})$;
  $Y_h \leftarrow Random(-\tau_{max}, \tau_{max})$;
  $\gamma_h \leftarrow Random(-\gamma_{max}, \gamma_{max})$;
  $s_i \leftarrow \{ID_i, X_h, Y_h, \gamma_h\}$;
  while $|X_h| > 0 \vee |Y_h| > 0$ **do**
    if $|X_h| > 0$ **then**
      Forward s_i to (X_h, Y_h) along X axis by one hop;
      $|X_h| = |X_h| - 1$;
    end if
    if $|Y_h| > 0$ **then**
      Forward s_i to (X_h, Y_h) along Y axis by one hop;
      $|Y_h| = |Y_h| - 1$;
    end if
  end while
  while $|\gamma_h| > 0$ **do**
    Forward s_i to γ along the identical-hop route by one hop;
    $|\gamma_h| = |\gamma_h| - 1$;
  end while
  Transmit s_i to sink node by least-hop routes;
end for

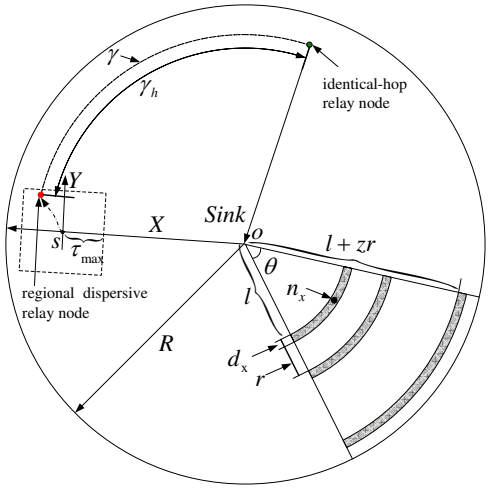

Fig. 2. Illustration of regional dispersive and disjoint identical-hop routings.

CPU, and all the sensor nodes are fairly treated in regional dispersive routing phase. Thus, the energy consumption of sensor nodes is not related to the sensor nodes' positions in these two operations. In the shortest path routing, sensor nodes close to the sink node aggregates the traffic of nodes far away from sink node, thus the insider sensor nodes consume more energy compared with outsider nodes. Thus, we analyze the energy consumption in least-hop routing phase to determine the available volume of redundant energy for hop length of shares transmission in disjoint identical-hop routing phase. Let R denote the radius of the network, r the transmission range, and λ the probability that packet transmission occurs. The energy consumption of each node can be obtained by the number of traffic transmissions, i.e., the number of transmitted shares.

Theorem 1: Let the distance from a sensor node to the sink node be l, $l = (h-1)r + x$, where x is the distance smaller than the distance of one hop. The number of transmitted shares relayed by this sensor node with the least-hop routing, denoted d_l, is

$$d_l = [(z+1) + \frac{z(z+1)r}{2l}]\lambda, \tag{5}$$

where z is any integer that can keep $l + zr < R$.

Proof. As shown in Fig. 2, node n_x is located at a district surrounded by sector radii and arcs, which consists of senor nodes with the identical hop length to the sink node. Let θ denote the angle of this sector, and d_x denote the height of this district. With the least-hop routing, the nodes in district relay all the traffic for the nodes with $l+r, l+2r, \cdots l+zr$ from the sink node in the sector. As we consider large scale high-density network, the length of d_x is infinitesimal and negligible. We can express the area of the district, $\theta l d_x$, and the number of the nodes in the district, $\rho\theta l d_x$. Thus, the number of shares transferred by the district is $\theta\rho l d_x\lambda$. The number of shares relayed by districts with $l + r, l + 2r, \cdots l+zr$ from the sink node in the sector can be deduced by analogy, which is $\theta\rho(l+zr)d_x\lambda$. Based on the number of transmitted shares in this sector, we can obtain the number of transmitted shares relayed by the sensor node n_x with the least-hop routing,

$$d_l = [\theta\rho l d_x + \theta(l+r)\rho d_x + \cdots + \theta(l+zr)\rho d_x]\lambda. \tag{6}$$

Reorganizing the eq. 6, the expression of d_l can be simplified as eq. 5. □

As the network lifetime depends on the first outage of sensor nodes, it is determined by the sensor node with the maximum energy consumption. Let d_{max} denote the transmitted number of shares by the node with the maximum energy consumption, and e_u the energy consumption for a share. The remaining energy for each sensor node is $(d_{max} - d_l)e_u$, which can be used for forwarding $(d_{max} - d_l)e_u/e_u$ hops along identical hop. Thus, the hop

length that can be forwarded along identical-hop routes is exactly $d_{max} - d_l$.

Theorem 2: The maximal hop length for a sensor node to forward along identical-hop route is $\min\{(d_{max} - d_l), \pi l\lambda/r\}$, where l_{min} is the minimal distance from the sink node to sensor nodes, and $d_{max} = [(z+1)+\frac{z(z+1)r}{2l_{min}}]\lambda$.

Proof. Based on Eq. 5, d_{max} can be expressed as $[(z+1)+\frac{z(z+1)r}{2l_{min}}]\lambda$. The remaining energy of each node is $(d_{max} - d_l)e_u$, which can support $(d_{max} - d_l)e_u/e_u = d_{max} - d_l$ hops forwarding along the identical-hop route without reducing the network lifetime. As each share can be forwarded along identical-hop route by two directions, the maximal length of routing path is half of the identical-hop circumference centered by the sink node, i.e., πl, and the maximal hop length along identical-hop route is $\pi l/r$. Thus, the maximal hop length for a sensor node to forward along identical-hop route is $\min\{(d_{max} - d_l), \pi l/r\}$. □

We define the whole-network dispersive routing to ensure that the disjoint identical-hop routing phase can be realized if the whole-network dispersive routing can be guaranteed. Whole-network dispersive routing is defined as the regional dispersive relay nodes can randomly forward the shares along the identical-hop routes all over the whole network without reducing the network lifetime. We derive the scale of the network for supporting whole-network dispersive routing.

Theorem 3: In order to support whole-network dispersive routing, we need to ensure that the least hop length of the WSNs' radius should be

$$z = \lceil \frac{R}{r} \rceil \geq \frac{\pi + \sqrt{\pi^2 + 4\pi}}{2} = 4, \text{where } z \text{ is integer.} \quad (7)$$

Proof. Intuitively, the redundant energy can support whole-network dispersive routing if it is enough to forward shares along identical-hop route by $\pi l\lambda/r$ hops. As all the shares are relayed by the neighbors of sink node, the difference between the energy of sink node's neighbors and other sensor nodes is the available energy. When $h = 0$, the available energy can support $(z+1+\frac{z(1+z)r}{2x})\lambda$ shares; When $h > 1$, the available energy can support $(z + 1 + \frac{z(1+z)r}{2(h-1)r+x})\lambda$ shares. The number of shares that remaining energy can support is denoted as ψ, which is

$$\psi = \frac{[z(1+z)r](h-1)r\lambda}{2x[(h-1)r+x]}. \quad (8)$$

The expression can be reorganized as

$$\frac{[z(1+z)r](h-1)r\lambda}{2x[(h-1)r+x]} \geq \frac{[z(1+z)](h-1)\lambda}{2h}. \quad (9)$$

To guarantee the whole-network dispersive routing, we should ensure the expectation of the available energy can be sufficient to forward shares by $\pi l\lambda/r < \pi h$ hops, where the expectation of the available energy is $[z(1+z)](h-1)\lambda/h$.

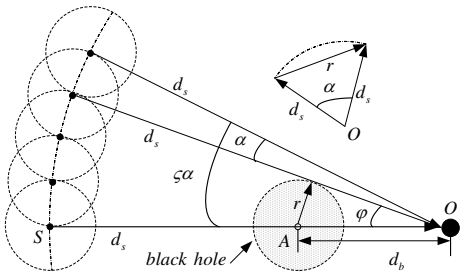

Fig. 3. Identical-hop routing under single black hole scenario.

Then, we can further derive the exact value of integer z:

$$\left.\begin{array}{l} \frac{[z(1+z)](h-1)\lambda}{h} > \pi h \\ h \leq z \end{array}\right\} \Rightarrow z \geq 4, \text{where } z \text{ is integer.} \quad (10)$$

□

Lemma 1: When the radius of WSNs is larger or equal to 4 hops, the whole-network dispersive routing does not reduce the network lifetime.

Proof. Based on Theorem 3, there will be enough redundant energy to support the whole-network dispersive routing, when the network radius is not less than 4. As the network lifetime depends on the sensor node with maximal energy consumption, the network lifetime is not decreased when there is enough redundant energy. □

V. ANALYSIS OF NETWORK SECURITY AND LIFETIME

In this section, we analyze the network security and lifetime of SEDR scheme. Firstly, single black hole case is considered, and the packet interception probability for single black hole is obtained in Subsection V-A. Then, we study the security performance of multiple black holes in Subsection V-B. Finally, the relationship between network lifetime and network security requirement is derived in Subsection V-C.

A. Security analysis for single black hole

Fig. 3 shows a single black hole system. d_s and d_b are denoted as the distance from the source node S, and compromised node A, to the sink node O, respectively. The compromised node usually pretends as a normal sensor node by black hole attack, thus it has the same capability as an ordinary sensor node, e.g., the transmission/attack range. Moreover, our analysis also considers the cases that the compromised nodes and ordinary sensor nodes have different capabilities [7], [25].

For one hop forwarding, let α denote the angle between source-sink line and destination-sink line, and φ is the angle

that the packets are captured by the black hole as shown in Fig. 3.

Theorem 4: In order to ensure that the black hole cannot intercept T shares when source node has sent M shares, the forwarding hop length, denoted ζ, should hold the following inequality in disjoint identical-hop routing phase:

$$\zeta > \lceil \frac{M \cdot \varphi}{T \cdot \alpha} \rceil = \lceil \frac{M \cdot \arcsin\left(\frac{r}{d_b}\right)}{T \cdot \arccos(\frac{2{d_s}^2 - r^2}{2{d_s}^2})} \rceil \tag{11}$$

Proof. For each hop, the angle $\alpha = \arccos[\frac{2{d_s}^2 - r^2}{2{d_s}^2}]$ according to the law of cosines. After ζ hops in disjoint identical-hop routing, the angle becomes $\zeta \cdot \alpha$. As proofed in [7], the worst case occurs when the center of black A, source node S and sink node O lie on the same line. We consider this worst case and assume that all the routes traverse through the black hole can be intercepted. Thus, all the routes within the angle $\varphi = \arcsin \frac{r}{d_b}$ can be captured by adversary, and the number of shares is $\frac{M \cdot \varphi}{\zeta \cdot \alpha}$. To ensure the security of packet transmission, the intercepted number of shares should be less than T, which is $\frac{M \cdot \varphi}{\zeta \cdot \alpha} < T$. Then, we can obtain the inequality of hop length ζ, in disjoint identical-hop routing to guarantee the security in Eq. 11. □

As the area around sink node is physically secured by the video monitoring equipments, sensor nodes located in the circular area, r_s, centered at sink node cannot be compromised. The cost and complexity of constructing video monitoring equipments highly depend on the size of the safe area r_s.

Theorem 5: When there is sufficient energy to operate whole-network dispersive routing, i.e., $z \geq 4$, the size of area r_s should fulfill the following inequality to guarantee the security.

$$r_s > \frac{r}{\sin\left\{\frac{T \cdot d_s \cdot \pi \cdot \arccos\left[(2{d_s}^2 - r^2)/(2{d_s}^2)\right]}{M \cdot r}\right\}} \tag{12}$$

Proof. When the available energy can support whole-network dispersive routing, we have $\zeta \leq \frac{d_s \cdot \pi}{r}$. Based on Theorem 4, the following inequality should be hold,

$$\frac{d_s \cdot \pi}{r} > \frac{M \cdot \arcsin\left(r/r_s\right)}{T \cdot \arccos\left[(2{d_s}^2 - r^2)/(2{d_s}^2)\right]}. \tag{13}$$

Then, we can get Eq. 12 by reorganizing Eq. 13. □

Theorem 6: The probability that each share may be intercepted by black hole is

$$\phi_1 = \frac{\varphi}{\zeta \alpha}. \tag{14}$$

Proof. When forwarded hop length of shares is ζ, $\varphi = \arcsin \frac{r}{d_b}$ and $\alpha = \arccos[(2{d_s}^2 - r^2)/(2{d_s}^2)]$. Based on the Theorem. 5, the probability is the occupied angle of the black hole over the angle of forwarded hop length, i.e., $\phi_1 = \frac{\varphi}{\zeta \alpha}$. □

Theorem 7: The packet interception probability of SEDR scheme under the scenario of single black hole, denoted as P_1, is

$$\begin{cases} P_1 = \sum_{j=T}^{M} C_M^j (\frac{\varphi}{\pi})^j (1 - \frac{\varphi}{\pi})^{(M-j)} \\ \text{where } \varphi = \arcsin\left(r/d_b\right). \end{cases} \tag{15}$$

Proof. As the SEDR scheme adopts the whole-network dispersive routing, shares are randomly and uniformly forwarded over the whole network. Thus, the probability that the black hole can intercept each share only depends on the occupied angle by the black hole in the whole network, which is φ/π. For the case that T shares are intercepted by the black hole, the probability is

$$P_1(T) = C_M^T (\frac{\varphi}{\pi})^T (1 - \frac{\varphi}{\pi})^{M-T}. \tag{16}$$

Thus, the probability of packet interception by the black hole is

$$P_1 = C_M^T (\frac{\varphi}{\pi})^T (1 - \frac{\varphi}{\pi})^{M-T} + \cdots + C_M^M (\frac{\varphi}{\pi})^M (1 - \frac{\varphi}{\pi})^0. \tag{17}$$

Reorganizing Eq. 17, we can obtain Eq. 15. □

Theorem 6 indicates the packet interception probability for each share. To correctly decode transmitted packet, the sink node requires at least T shares.

Lemma 2: To ensure that at least T shares are not intercepted by the black hole, the least required number of transmitted shares M should be

$$M \geq \lceil \frac{T}{1 - \phi_1} \rceil, \text{ where } \phi_1 = \frac{\varphi}{\zeta \alpha} \tag{18}$$

Proof. According to Theorem 6, the packet interception probability is $\phi_1 = \frac{\varphi}{\zeta \alpha}$. Thus, the least required number of transmitted shares M should be $(1 - \phi_1)M \geq T$, which is $M \geq \lceil \frac{T}{1 - \phi_1} \rceil$. □

On the other hand, to prevent adversary decoding the packet, the number of received shares by black hole should be less than T.

Lemma 3: To guarantee the number of intercepted shares by black hole to be less than T, the number of transmitted shares M should be

$$M \leq \lfloor \frac{T}{\phi_1} \rfloor, \text{ where } \phi_1 = \frac{\varphi}{\zeta \alpha}. \tag{19}$$

Proof. Based on Theorem 6, the packet interception probability is $\phi_1 = \frac{\varphi}{\zeta \alpha}$. Thus, the probability that T shares are intercepted by the black hole is $M\phi_1$. To ensure that the number of eavesdropped shares is less than T, we should guarantee $M\phi_1 < T$, i.e., $M \leq \lfloor \frac{T}{\phi_1} \rfloor$. □

From Lemmas 2 and 3, the security of packet can be guaranteed only when at least T shares are received by the sink node and less than T shares are intercepted by the black hole.

Definition For each packet, if and only if the sink node can receive at least T shares and less than T shares are intercepted by the black hole, the bi-security of the packet is guaranteed.

Intuitively, the packet can be successfully decoded by the sink node without being acquired by the adversary if and only if bi-security of the packet can be guaranteed.

Lemma 4: To ensure the security of a packet,

$$\phi_1 = \frac{\varphi}{\zeta\alpha} = \frac{\arcsin(r/d_b)}{\zeta \cdot \arccos[(2{d_s}^2 - r^2)/(2{d_s}^2)]} < 0.5 \quad (20)$$

Proof. According to Lemmas 2 and 3, to ensure the bi-security of a packet, we have $\phi_1 \leq 1 - T/M$ and $\phi_1 < T/M$, i.e., $\phi_1 < \min\{(1-T/M), T/M\}$. If $T/M > 0.5$, we have $\phi_1 < 0.5$; If $T/M < 0.5$, we also have $\phi_1 < 0.5$. Thus, ϕ_1 is always smaller than 0.5. □

Based on the definition of bi-security of a packet, we derive the minimal size of the physically secured area as follows.

Theorem 8: To ensure the bi-security of a packet, the minimal physically secured area under bi-security requirement of SEDR scheme, denoted ${r_s}^*$, should ensure

$${r_s}^* > \begin{cases} \frac{r}{\sin[\frac{T d_s \pi \alpha}{M r}]}, & \frac{T}{M} \leq 0.5 \\ \frac{r}{\sin[(1-\frac{T}{M})\frac{d_s \pi \alpha}{r}]}, & \frac{T}{M} > 0.5. \end{cases} \quad (21)$$

Proof. According to Lemma 4, we have

$$\phi_1 = \begin{cases} \frac{\varphi}{\zeta\alpha} < \frac{T}{M}, & \frac{T}{M} < 0.5 \\ \frac{\varphi}{\zeta\alpha} \leq 1 - \frac{T}{M}, & \frac{T}{M} \geq 0.5 \end{cases} \quad (22)$$

By substituting $\zeta = \frac{d_s \pi}{r}$ and ${r_s}^*$ into Eq. 22, we can obtain Eq. 21. □

Similarly, we can obtain the minimal physically secured area under bi-security requirement of I-walk, namely ${r_s}^0$.

$${r_s}^0 > \begin{cases} \frac{r}{\sin[\frac{T\zeta}{M}\arccos(\frac{2R^2 - r^2}{2R^2})]}, & \frac{T}{M} \leq 0.5 \\ \frac{r}{\sin[(1-\frac{T}{M})\zeta\arccos(\frac{2R^2 - r^2}{2R^2})]}, & \frac{T}{M} > 0.5, \end{cases} \quad (23)$$

where R is the radius of the WSNs.

Lemma 5: The cost of constructing physically secured area of SEDR scheme never exceeds the cost of I-walk's.

Proof. Since $d_s\pi/r$ is not less than ζ and $\alpha = \arccos[(2{d_s}^2 - r^2)/(2{d_s}^2)] \geq \arccos[(2R^2 - r^2)/(2R^2)]$, we have ${r_s}^* \leq {r_s}^0$. Therefore, the cost of constructing physically secured area of SEDR scheme is at most the same as that of I-walk. □

B. Security analysis for multiple black holes

As we consider large-scale high-density WSNs, there may exist several black holes in the network at the same time. Based on the results in Subsection. V-A, we further analyze the security performance under scenario of multiple black holes. We assume that the adversaries always choose the best position to establish black holes, i.e., the center of black holes, identical-hop relay node and sink node are on the same line. The parameters defined in the scenario of multiple black holes are the same as those in single black hole case. Suppose there are k black holes in the network and all black holes have the same size.

Theorem 9: The probability for each share to traverse through black holes under the scenario of k black holes is

$$\phi_k = \min(\frac{k\varphi}{\zeta\alpha}, 1). \quad (24)$$

Proof. From Theorem. 4, the occupied angle of one black hole is 2φ. Thus, for k black holes, the maximal occupied angle is $2k\varphi$. Then, we can obtain the probability for each share to traverse through black holes as $P^k = \min(2k\varphi/2\zeta\alpha, 1)$, which is Eq. 24. □

Based on Theorem. 9, we can derive the packet interception probability of the adversaries under the scenario of k black holes.

Lemma 6: The probability that the packet can be successfully decoded by the adversaries is

$$P_k = \begin{cases} \sum_{j=T}^{M} C_M^j (\frac{k\varphi}{\pi})^j (1 - \frac{k\varphi}{\pi})^{(M-j)}, & k\varphi < \pi \\ 1, & k\varphi \geq \pi \end{cases} \quad (25)$$

Proof. For k black holes, the maximal occupied angle in the whole network is $\min(2k\varphi, 2\pi)$. If the total occupied angle is not less than 2π, all the shares will be received by the adversaries, thus the packet interception probability P_k is 1; Otherwise, the occupied angle is $2k\varphi$, and the probability that at least T shares are intercepted by the adversaries is

$$P_k = \sum_{j=T}^{M} C_M^j (\frac{k\varphi}{\pi})^j (1 - \frac{k\varphi}{\pi})^{(M-j)}. \quad (26)$$

Combining both cases, we have Eq. 26. □

We have obtained the probability that the adversaries can successfully acquire the transmitted packet for the case that the adversaries always compromise the nodes located in the best positions. We further derive the packet interception probability for the case that black holes are randomly distributed in the whole network.

Theorem 10: Suppose k black holes are uniformly and randomly distributed in the network region with radius R. If black holes do not overlap with each other, the packet interception probability, denoted P_k^u, is

$$\begin{cases} P_k^u = C_M^T \eta^T (1-\eta)^{(M-T)} \\ \text{where } \eta = \int_0^R \frac{\arcsin(r/x)}{\pi} \frac{2x}{R^2} \, \mathrm{d}x. \end{cases} \quad (27)$$

Proof. Firstly, we consider the case that there is only one black hole in the network, and the probability density function that the black hole located at the position which is x far away from the sink node can be expressed as

$$f_x = \begin{cases} \frac{2x}{R^2}, & 0 < x < R \\ 0, & \text{otherwise.} \end{cases} \tag{28}$$

Thus, the packet interception probability for the case of single randomly distributed black hole, P_1^u, is

$$P_1^u = \int_0^R f_x \frac{\arcsin(r/x)}{\pi} \, \mathrm{d}x = \int_0^R \frac{2x}{R^2} \frac{\arcsin(r/x)}{\pi} \, \mathrm{d}x. \tag{29}$$

Similar to previous derivation, we can obtain the packet interception probability that at least T packets are intercepted, when k non-overlapping black holes are established. □

C. Network lifetime analysis

In this subsection, we consider the scenario that there are k black holes. The adversaries can always choose the best positions to establish black holes, i.e., the center of black holes, identical-hop relay node and sink node are on the same line. We analyze the impact of packet interception probability on network lifetime, and try to establish the relationship between packet interception probability and network lifetime.

Theorem 11: For the same WSNs and routing strategy, let the packet interception probability be $P_k(x_1)$ and $P_k(x_2)$, and $P_k(x_1) < P_k(x_2)$. The ratio of network lifetime to achieve the same security requirement in these two cases is $\lceil \frac{1}{1-P_k(x_1)} \rceil / \lceil \frac{1}{1-P_k(x_2)} \rceil$.

Proof. According to Theorem. 3, the least required number of shares M should exceed $\lceil \frac{T}{1-P_k} \rceil$. As the initial network energy of sensor nodes and the routing strategy are the same, the ratio of network lifetime to guarantee the same network security level equals the inverse of the ratio of least required number of shares, which is $\lceil \frac{1}{1-P_k(x_1)} \rceil / \lceil \frac{1}{1-P_k(x_2)} \rceil$. □

VI. SIMULATION RESULTS

Our simulation is conducted by OMNET++, which is an open network simulation platform for large network [33]. Our WSNs are a circular region with radius $400m$, which consists of 800 sensor nodes evenly distributed in the network. The traffic is randomly and evenly generated for each node. Detail of simulation configurations is shown in Table II. We study the impact of source-sink distance d_s, the distance between compromised node and sink node d_b, the spreading hop length ζ, and the number of black holes in Fig. 4, Fig. 5, Fig. 6, and Fig. 7, respectively. Fig. 4 shows the black hole interception probability with different source-sink distances when the distance between the sink node and black hole is fixed at $50m$. For I-walk routing, the packet interception probability increases with the increase of source-sink distance. For SEDR scheme, the packet interception probability can be determined by angle φ without being changed by the source-sink distance d_s, since shares are routed all over the network. Fig. 5 and Fig. 6 show the packet interception probability with different locations of black hole and the spreading hop length ζ, respectively. Obviously, when black hole's location is faraway from sink or shares are spread faraway from source node, the probability of packet interception is decreased, which leads to better performance of security. We further evaluate the security performance of SEDR against I-walk under multiple black holes as shown in Fig. 7. We can see our SEDR scheme has lower packet interception probability and the simulation results are consistent with theoretical one. Overall, all these figures show that: i) the simulation results match our theoretical analysis, and ii) SEDR scheme significantly outperforms the I-walk with different parameters in security.

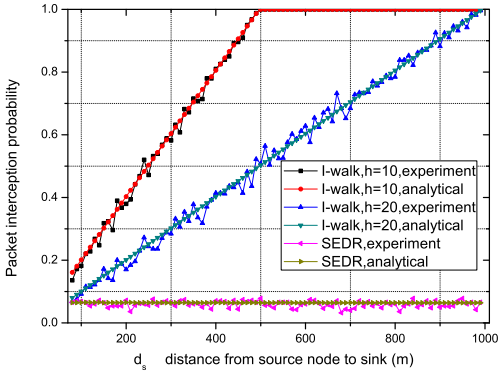

Fig. 4. Impact of source-sink distance on packet interception probability.

TABLE II
SIMULATION CONFIGURATIONS

System configuration for simulation	
Number of Sensor Nodes	800
Network Radius R (m)	400 m
Distance Threshold d_0 (m)	87 m
Sensing Range (m)	15 m
Energy losses E_c (nJ/bit)	50 nJ/bit
$\mathcal{E}_{fs}$ (pJ/bit/m^2)	10 pJ/bit/m^2
$\mathcal{E}_{amp}$ (pJ/bit/m^4)	0.0013 pJ/bit/m^4
Initial energy (J)	0.5 J

Table III shows the least required number of shares M needed to be transmitted under the case that at least $T = 4$ shares are received by the sink node to decode the packet. It is found that the least required number of shares M climbs with the increase of d_s. Since the outage of network highly

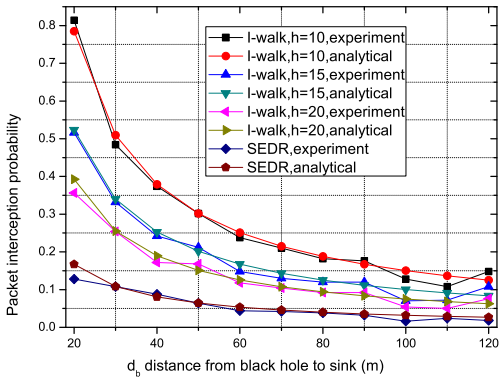

Fig. 5. Impact of black holes' locations on packet interception probability.

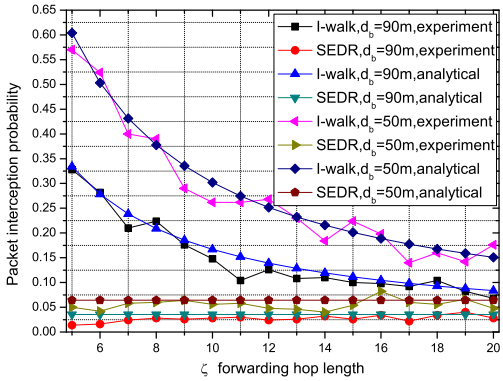

Fig. 6. Impact of forwarded hop length on packet interception probability.

depends on the number of shares M, our simulations are conducted to evaluate the total energy consumption and network lifetime of proposed SEDR scheme with various transmission range r in Fig. 8 and Fig. 9, respectively. It can be seen from Fig. 8, when transmission range r is relatively small, I-walk consumes more energy than the SEDR due to more transmission of shares; when transmission range r is relatively large, the proposed SEDR has higher energy

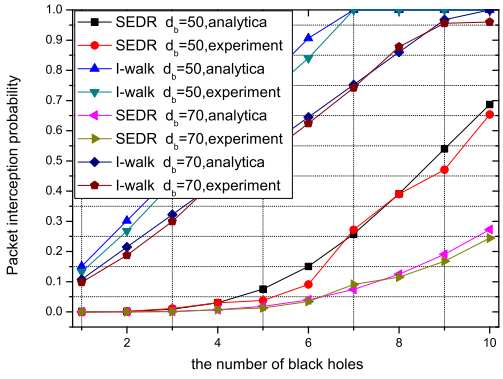

Fig. 7. Impact of black holes' number on packet interception probability.

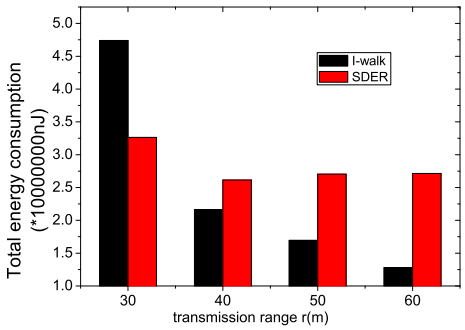

Fig. 8. Impact of transmission range on total energy consumption.

consumption comparing with I-walk due to utilizing the redundant energy to forward the shares. Fig. 9 shows the network lifetime for rounds of packet transmissions with different value of r. The SEDR always outperforms I-walk with the same security requirement, since the shares transmitted by the SEDR have lower probability to be intercepted by the adversary, which leads to a lower required number of shares M and releases the burden of the sensor node with maximal energy consumption.

TABLE III
LEAST REQUIRED SHARE NUMBER M WITH VARIOUS PARAMETERS

Transmission Range (r)	Black Hole Location (d_b)	Source-sink Distance (d_s)	Least Number of Shares (M)
30	150	< 150	5
		< 240	6
		< 420	7
		< 550	8
		< 600	9
40	200	< 200	5
		< 330	6
		< 560	7
		< 600	8
50	250	< 250	5
		< 410	6
		< 600	7
60	300	< 300	5
		< 490	6
		< 600	7

VII. CONCLUSION

In this paper, we have studied the problem of secret sharing based multi-path routing and formulated it as an optimization problem to maximize both the network security and lifetime. Based on secret sharing technique, the SEDR scheme has been proposed to deliver sliced shares to the sink node with randomized disjoint multi-path routes by

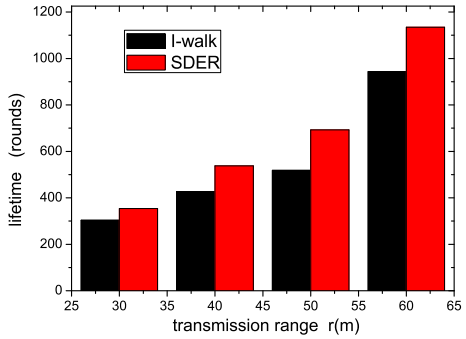

Fig. 9. Impact of transmission range on network lifetime.

utilizing the available surplus energy of sensor nodes, such that the network security is maximized without decreasing the lifetime of WSNs. Theoretical analysis and extensive simulation results show that the SEDR scheme outperforms I-walk in both network security and lifetime under various parameters. In our future work, we will design energy-efficient and secure routing scheme for wireless sensor networks considering both packet loss and delay due to fading channel.

REFERENCES

[1] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, 2009.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

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

[4] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1501–1514, 2009.

[5] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. T. Abdelzaher, "Pda: Privacy-preserving data aggregation in wireless sensor networks," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, 2007, pp. 2045–2053.

[6] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[7] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941–954, 2010.

[8] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[9] M. Kim, E. Jeong, Y. C. Bang, S. Hwang, and B. Kim, "Multipath energy-aware routing protocol in wireless sensor networks," in *Proc. IEEE INSS*, Kanazawa, JP, 2008, pp. 127–130.

[10] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1380–1397, 2011.

[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, pp. 293–315, 2003.

[12] H. M. Sun, C. M. Chen, and Y. C. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in *Proc. IEEE TENCON*, Taipei, Taiwan, 2007, pp. 1–4.

[13] D. B. Johnson, D. A. Maltz, and J. Broch, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139–172, 2001.

[14] M. K. Marina and S. R. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. IEEE ICNP*, Riverside, CA, USA, 2001, pp. 14–23.

[15] Z. Ye, V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, San Franciso, CA, USA, 2003, pp. 270–280.

[16] W. Lou, W. Liu, and Y. Fang, "Spread: Enhancing data confidentiality in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Hong Kong, CN, 2004., pp. 2404–2413.

[17] W. Lou and Y. Kwon, "H-spread: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," *IEEE Transactions Vehicular Technology*, vol. 55, no. 4, pp. 1320–1330, 2006.

[18] P. Papadimitratos and Z. J. Haas, "Secure data communication in mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 343–356, 2006.

[19] D. C. Dhanapala, A. P. Jayasumana, and Q. Han, "On random routing in wireless sensor grids: A mathematical model for rendezvous probability and performance optimization," *Journal of Parallel and Distributed Computing*, vol. 71, no. 3, pp. 369–380, 2011.

[20] H. Shokrzadeh, A. T. Haghighat, and A. Nayebi, "New routing framework base on rumor routing in wireless sensor networks," *Computer Communications*, vol. 32, no. 1, pp. 86–93, 2009.

[21] H. Shokrzadeh, M. Mashaiekhi, and A. Nayebi, "Improving directional rumor routing in wireless sensor networks," in *Proc. IEEE IIT*, Dubai, AE, 2007, pp. 108–112.

[22] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[23] T. Banka, G. Tandon, and A. P. Jayasumana, "Zonal rumor routing for wireless sensor networks," in *Proc. IEEE ITCC*, Las Vegas, NV, USA, 2005, pp. 562–567.

[24] A. F. Liu, P. H. Zhang, and Z. G. Chen, "Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 71, no. 10, pp. 1327–1355, 2011.

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

[26] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications.*, vol. 24, no. 4, pp. 829–835, 2006.

[27] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE SP*, Oakland, CA, USA, 2003, pp. 197–213.

[28] S. Samarah, M. Al-Hajri, and A. Boukerche, "A predictive energy-efficient technique to support object-tracking sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 656–663, 2011.

[29] D. R. Stinson, *Cryptography, Theory and Practice*, D. R. Stinson, Ed. CRC Press, 2006.

[30] J. Lian, K. Naik, and G. B. Agnew, "Data capacity improvement of wireless sensor networks using non-uniform sensor distribution," *International Journal of Distributed Sensor Networks*, vol. 2, no. 2, pp. 121–145, 2006.

[31] S. He, J. Chen, Y. Sun, D. K. Y. Yau, and N. K. Yip, "On optimal information capture by energy-constrained mobile sensors," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2472–2484, 2010.

[32] Y. Chen and Q. Zhao, "On the lifetime of wireless sensor networks," *IEEE Communications Letters*, vol. 9, no. 11, pp. 976–978, 2005.

[33] Omnet++ network simulation framework http://www.omnetpp.org/. [Online]. Available: http://www.omnetpp.org/