Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks

Di Tang Tongtong Li Jian Ren Jie Wu

***Abstract*—Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenishable energy resources. In this paper, we first propose a novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic-based random walking. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, we propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. We also provide a quantitative security analysis on the proposed routing protocol. Our theoretical analysis and OPNET simulation results demonstrate that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, our analysis shows that we can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. We also demonstrate that the proposed CASER protocol can achieve a high message delivery ratio while preventing routing traceback attacks.**

***Index Terms*—routing, security, energy efficiency, energy balance, delivery ratio, deployment, simulation**

I. Introduction

The recent technological advances make wireless sensor networks (WSNs) technically and economically feasible to be widely used in both military and civilian applications, such as monitoring of ambient conditions related to the environment, precious species and critical infrastructures. A key feature of such networks is that each network consists of a large number of untethered and unattended sensor nodes. These nodes often have very limited and non-replenishable energy resources, which makes energy an important design issue for these networks.

Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime.

In addition to the aforementioned issues, WSNs rely on wireless communications, which is by nature a broadcast medium. It is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In particular, in the wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor network communications. The adversaries may use expensive radio transceivers, powerful workstations and interact with the network from a distance since they are not restricted to using sensor network hardware. It is possible for the adversaries to perform jamming and routing traceback attacks.

Motivated by the fact that WSNs routing is often geography-based, we propose a geography-based secure and efficient Cost-Aware SEcure routing (CASER) protocol for WSNs without relying on flooding. CASER allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. The distribution of these two strategies is determined by the specific security requirements. This scenario is analogous to delivering US Mail through USPS: express mails cost more than regular mails; however, mails can be delivered faster. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. In addition, we also give quantitative secure analysis on the proposed routing protocol based on the criteria proposed in [1].

CASER protocol has two major advantages: (i) It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized. (ii) CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing traceback attacks and malicious traffic jamming attacks in WSNs.

Our contributions of this paper can be summarized as follows:

1) We propose a secure and efficient Cost-Aware SEcure Routing (CASER) protocol for WSNs. In this protocol, cost-aware based routing strategies can be applied to address the message delivery requirements.
2) We devise a quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are maximized under the same energy deployment.
3) We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control and security requirements.
4) We quantitatively analyze security of the proposed rout-

Di Tang, Tongtong Li and Jian Ren are with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824-1226. Email: {ditony, tongli, renjian}@egr.msu.edu.

Jie Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122. Email: jiewu@temple.edu.

ing algorithm.

5) We provide an optimal non-uniform energy deployment strategy for the given sensor networks based on the energy consumption ratio. Our theoretical and simulation results both show that under the same total energy deployment, we can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario.

The rest of this paper is organized as follows. In Section II, the related work is reviewed. The system model is presented in Section III. The proposed scheme is described in Section IV. In Section VI, security analysis of the proposed scheme is conducted. Section VII provides performance analysis of the proposed scheme. We present the optimal, non-uniform energy deployment strategy for CASER in Section VIII. We conclude in Section IX.

II. Related Work

Routing is a challenging task in WSNs due to the limited resources. Geographic routing has been widely viewed as one of the most promising approaches for WSNs. Geographic routing protocols utilize the geographic location information to route data packets hop-by-hop from the source to the destination [2]. The source chooses the immediate neighboring node to forward the message based on either the direction or the distance [3]–[6]. The distance between the neighboring nodes can be estimated or acquired by signal strengths or using GPS equipments [7], [8]. The relative location information of neighbor nodes can be exchanged between neighboring nodes.

In [5], a geographic adaptive fidelity (GAF) routing scheme was proposed for sensor networks equipped with low power GPS receivers. In GAF, the network area is divided into fixed size virtual grids. In each grid, only one node is selected as the active node, while the others will sleep for a period to save energy. The sensor forwards the messages based on greedy geographic routing strategy. A query based geographic and energy aware routing (GEAR) was proposed in [6]. In GEAR, the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighboring nodes based on estimated cost and learning cost. The estimated cost considers both the distance to the destination and the remaining energy of the sensor nodes. While the learning cost provides the updating information to deal with the local minimum problem.

While geographic routing algorithms have the advantages that each node only needs to maintain its neighboring information, and provides a higher efficiency and a better scalability for large scale WSNs, these algorithms may reach their local minimum, which can result in dead end or loops. To solve the local minimum problem, some variations of these basic routing algorithms were proposed in [9], including GEDIR, MFR and compass routing algorithm. The delivery ratio can be improved if each node is aware of its 2-hop neighbors. There are a few papers [3], [10]–[12] discussed combining greedy and face routing to solve the local minimum problem. The basic idea is to set the local topology of the network as a planar graph, and then the relay nodes try to forward messages along one or possibly a sequence of adjacent faces toward the destination.

Lifetime is another area that has been extensively studied in WSNs. In [13], a routing scheme was proposed to find the sub-optimal path that can extend the lifetime of the WSNs instead of always selecting the lowest energy path. In the proposed scheme, multiple routing paths is set ahead by a reactive protocol such as AODV or directed diffusion. Then, the routing scheme will choose a path based on a probabilistic method according to the remaining energy. In [14], the authors assumed that the transmitter power level can be adjusted according to the distance between the transmitter and the receiver. Routing was formulated as a linear programming problem of neighboring node selection to maximize the network lifetime. Then [15] investigated the unbalanced energy consumption for uniformly deployed data-gathering sensor networks. In this paper, the network is divided into multiple corona zones and each node can perform data aggregation. A localized zone-based routing scheme was proposed to balance energy consumption among nodes within each corona. The authors in [16] formulated the integrated design of route selection, traffic load allocation, and sleep scheduling to maximize the network lifetime. Based on the concept of opportunistic routing, [17] developed a routing metric to address both link reliability and node residual energy. The sensor node computes the optimal metric value in a localized area to achieve both reliability and lifetime maximization.

In addition, exposure of routing information presents significant security threats to sensor networks. By acquisition of the location and routing information, the adversaries may be able to traceback to the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design [18]–[20].

In [21], source-location privacy is provided through broadcasting that mixes valid messages with dummy messages. The main idea is that each node needs to transmit messages consistently. Whenever there is no valid message to transmit, the node transmits dummy messages. The transmission of dummy messages not only consumes significant amount of sensor energy, but also increases the network collisions and decreases the packet delivery ratio. In phantom routing protocol [22], each message is routed from the actual source to a phantom source along a designed directed walk through either sector-based approach or hop-based approach. The direction/sector information is stored in the header of the message. Then every forwarder on the random walk path forwards this message to a random neighbor based on the direction/sector determined by the source node. In this way, the phantom source can be away from the actual source. Unfortunately, once the message is captured on the random walk path, the adversaries is able to get the direction/sector information stored in the header of the message. Therefore, exposure of the direction decreases the complexity for adversaries to trace back to the actual message source in the magnitude of 2^h.

In [19], [20], we developed a two-phase routing algorithm to provide both content confidentiality and source-location privacy. The message is first transmitted to a randomly selected intermediate node in the sensor domain before the message is being forwarded to a network mixing ring where the messages from different directions are mixed. Then the message is forwarded from the ring to the sink node. In [1], we developed criteria to quantitatively measure source-location information leakage for routing-based schemes through source-location disclosure index (SDI) and source-location space index (SSI). To the best of our knowledge, none of these schemes have considered privacy from a cost-aware perspective.

In this paper, for the first time, we propose a secure and efficient Cost-Aware SEcure Routing (CASER) protocol that can address energy balance and routing security concurrently in WSNs. In CASER protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design tradeoff between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries. Our extensive OPNET simulation results show that CASER can provide excellent energy balance and routing security. It is also demonstrated that the proposed secure routing can increase the message delivery ratio due to reduced dead ends and loops in message forward.

III. Models and Assumptions

A. The System Model

We assume that the WSNs are composed of a large number of sensor nodes and a sink node. The sensor nodes are randomly deployed throughout the sensor domain. Each sensor node has a very limited and non-replenishable energy resource. The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy. The information of the sink node is made public. For security purposes, each message may also be assigned a node ID corresponding to the location where this message is initiated. To prevent adversaries from recovering the source location from the node ID, a dynamic ID can be used. The content of each message can also be encrypted using the secret key shared between the node/grid and the sink node.

We also assume that each sensor node knows its relative location in the sensor domain and has knowledge of its immediate adjacent neighboring grids and their energy levels of the grid. The information about the relative location of the sensor domain may be broadcasted in the network for routing information update.

In this paper, we will not deal with key management, including key generation, key distribution and key updating.

B. The Adversarial Model and Assumptions

In WSNs, the adversary may try to recover the message source or jam the message from being delivered to the sink node. The adversaries would try their best to equip themselves with advanced equipments, which means they would have some technical advantages over the sensor nodes. In this paper, the adversaries are assumed to have the following characteristics:

- The adversaries will have sufficient energy resources, adequate computational capability and enough memory for data storage. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. They can move to this sender's location without too much delay. They may also compromise some sensor nodes in the network.
- The adversaries will not interfere with the proper functioning of the network, such as modifying messages, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping on the communications.
- The adversaries are able to monitor the traffic in any specific area that is important for them and get all of the transmitted messages in that area. However, we assume that the adversaries are unable to monitor the entire network. In fact, if the adversaries could monitor the entire WSN, they can monitor the events directly without relying on other people's sensor network.

C. Design Goals

Our design goal can be summarized as follows:

- To maximize the sensor network lifetime, we ensure that the energy consumption of all sensor grids are balanced.
- To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping when an alternative routing path exists.
- The adversaries should not be able to get the source location information by analyzing the traffic pattern.
- The adversaries should not be able to get the source location information if he is only able to monitor a certain area of the WSN and compromise a few sensor nodes.
- Only the sink node is able to identify the source location through the message received. The recovery of the source location from the received message should be very efficient.
- The routing protocol should maximize the probability that the message is being delivered to the sink node when adversaries are only able to jam a few sensor nodes.

D. Overview of the Proposed Scheme

In our scheme, the network is evenly divided into small grids. Each grid has a relative location based on the grid information. The node in each grid with the highest energy level is selected as the head node for message forwarding. In addition, each node in the grid will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighboring grids. The information maintained by each sensor node will be updated periodically.

We assume that the sensor nodes in its direct neighboring grids are all within its direct communication range. We also assume that the whole network is fully connected through multi-hop communications.

While maximizing message source location privacy and minimizing traffic jamming for communications between the source and the destination nodes, we can optimize the sensor network lifetime through a balanced energy consumption throughout the sensor network.

In addition, through the maintained energy levels of its adjacent neighboring grids, it can be used to detect and filter out the compromised nodes for active routing selection.

IV. The Proposed CASER Routing Protocol

We now describe the proposed CASER protocol. Under the CASER protocol, routing decisions can vary to emphasize different routing strategies. In this paper, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention. As described before, we are interested in routing schemes that can balance energy consumption.

A. Assumptions and Energy Balance Routing

In the CASER protocol, we assume that each node maintains its relative location and the remaining energy levels of its immediate adjacent neighboring grids. For node A, denote the set of its immediate adjacent neighboring grids as $\mathcal{N}_A$ and the remaining energy of grid i as $\mathcal{E}r_i$, $i \in \mathcal{N}_A$. With this information, the node A can compute the average remaining energy of the grids in $\mathcal{N}_A$ as $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.

In the multi-hop routing protocol, node A selects its next hop grid only from the set $\mathcal{N}_A$ according to the predetermined routing strategy. To achieve energy balance among all the grids in the sensor network, we carefully monitor and control the energy consumption for the nodes with relatively low energy levels by configuring A to only select the grids with relatively higher remaining energy levels for message forwarding.

For this purpose, we introduce a parameter $\alpha \in [0, 1]$ to enforce the degree of the *energy balance control (EBC)*. We define the candidate set for the next hop node as $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$ based on the EBC α. It can be easily seen that a larger α corresponds to a better EBC. It is also clear that increasing of α may also increase the routing length. However, it can effectively control energy consumption from the nodes with energy levels lower than $\alpha\mathcal{E}_a(A)$.

We summarize the CASER routing protocol in Algorithm 1. It should be pointed out that the EBC parameter α can be configured in the message level, or in the node level based on the application scenario and the preference. When α increases from 0 to 1, more and more sensor nodes with relatively low energy levels will be excluded from the active routing selection. Therefore, the $\mathcal{N}_A^\alpha$ shrinks as α increases. In other words, as α increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since $\mathcal{E}_a(A)$ is defined as the average energy level of the nodes in $\mathcal{N}_A$, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from $\mathcal{N}_A^\alpha$.

Algorithm 1 Node A finds the next hop routing grid based on the EBC $\alpha \in [0, 1]$

```
Compute the average remaining energy of the adjacent neighboring grids: $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.
Determine the candidate grids for the next routing hop: $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$.
Send the message to the grid in the $\mathcal{N}_A^\alpha$ that is closest to the sink node based on its relative location.
```

1) Probability Analysis: The parameter EBC enforces the route to bypass the grids with lower remaining energy levels to extend the lifetime of network. To analyze the effect, the network is divided into small grids, as shown in Fig. 1. When the source node has a message to forward to the sink node, the source node selects a relay grid from its neighbor grids based on both hop distance and the remaining energy level. We divide the entire sensor domain into four $\frac{\pi}{2}$ sections i $(i = 1, 2, 3, 4)$ corresponding to F(orward), U(pper), D(own) and B(ackward). The distance from the section G_i to the sink node is denoted as d_i. We also denote the remaining energy level of section i as $\mathcal{E}_i$ $(i = 1, 2, 3, 4)$. Since the initial energy distribution each grids and the events distribution are both random variables, the remaining energy level $\mathcal{E}_i$ is also a random variable and independent and identically distributed (iid). Let $f(e_i)$ be the probability distribution function (PDF) of $\mathcal{E}_i$. Based on Algorithm 1 and remaining energy distribution, the probability that section i is not selected as a candidate direction can be derived as follows:

$$\begin{aligned} P(Z_i) &= P\left(\mathcal{E}_i < \alpha \times \frac{\Sigma_{i=1}^4\mathcal{E}_i}{4}\right) \\ &= P\left(\frac{4\cdot\mathcal{E}_i}{\alpha} - \Sigma_{i=1}^4\mathcal{E}_i < 0\right),\ i = 1, \cdots, 4, \quad (1) \end{aligned}$$

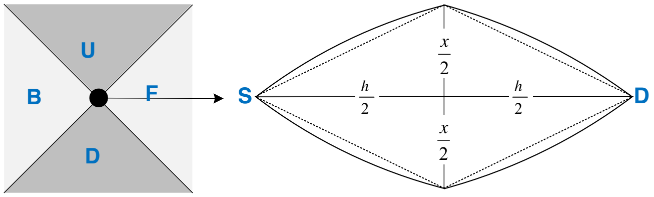
where Z_i is the event that grid G_i is not selected as the candidate grid due to its relatively low remaining energy level.

Denote P_i as the probability that grid G_i is selected as the relay grid for message forwarding. Suppose $d_1 \leq ... \leq d_4$, then we have

$$P_i = \prod_{j=1}^{i-1} P(Z_j)\cdot[1 - P(Z_i)],\ i = 1, \cdots, 4, \quad (2)$$

where $P(Z_i) = \int_{-\infty}^{0} f(z_i)\,dz_i$, and $f(z_i)$ is the PDF of random variable Z_i.

2) Analysis on energy distribution: Assume that each sensor node is initially deployed with equal initial energy. The energy level decreases when the sensor node forwards message. The remaining energy level of each node is based on the events distribution. Since the event is a random variable in the network, we assume the remaining energy levels of the sensor nodes are iid random variables.



(a) Next hop node distribution

(b) Routing path

Fig. 1. Routing path and length estimation.

Since the network is randomly deployed, the number of sensor nodes in each grid is determined by the size of the grid. So the number of sensor nodes in each grid also follows iid. We assume that the number of sensor nodes in each grid is large enough so that the initial energy of each girds should follows the normal distribution according to the central limit theorem. For each layer, the energy consumption for sensing and forwarding also follow the normal distribution. So the remaining energy level $\mathcal{E}_i$ shall follow the normal distribution, that is $\mathcal{E}_i \sim N(\mu_i, \sigma_i^2)$, where μ_i is the mean of the remaining energy level of each grid, σ_i is the standard derivation of energy distribution. Then

$$Z_i \sim N\left(\mu_i', \sigma_i'^2\right), \tag{3}$$

$$f(Z_i) = \frac{1}{\sqrt{2\pi}\sigma_i'} e^{-\frac{1}{2}\frac{(z_i-\mu_i')^2}{\sigma_i'^2}}, \tag{4}$$

$$P(Z_i) = \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi}\sigma_i'} e^{-\frac{1}{2}\frac{(z_i-\mu_i')^2}{\sigma_i'^2}} dz_i, \tag{5}$$

where $\mu_i' = \frac{4}{\alpha}\mu_i - \Sigma_{j=1}^4 \mu_j$ and $\sigma_i'^2 = (\frac{4}{\alpha}-1)^2\sigma_i^2 + \Sigma_{j=1,j\neq i}^4 \sigma_j^2$.

3) The hop distance estimation: As shown in Fig. 1, we divide the whole sensor domain into four equal size sections F, B, U and D. Let P_F, P_B, P_U and P_D be the probabilities that the message is forwarded to the sections F, B, U and D, respectively. Then we have the following theorem.

Theorem 1. *Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then the number of routing hops in the dynamic routing protocol can be estimated by the following equation*

$$\frac{h\sqrt{1+\left(\frac{P_U+P_L}{P_F-P_B}\right)^2}}{P_F-P_B}. \tag{6}$$

where h is the shortest hop distance between the source and the sink.

Proof: Since the network is randomly deployed, the number of sensor nodes in each grid is determined by the size of the grid. So the number of sensor nodes in each grid follows iid. When the number of sensor nodes in each grid is large enough, the sum of the energy in each grid should follow the normal distribution according to the central limit theorem. Therefore, the energy consumption for each grid is also the iid and follows the normal distribution.

In dynamic routing algorithm, the next forwarding node is selected based on the routing protocol. As shown in Fig. 1, since the probability of P_U and P_D have similar effect, while the $P_F - P_B$ needs to move the message forward h hops, therefore we have estimation $(P_F - P_B) : (P_U + P_D) = h : x$, where x is the routing hops that the message is routed in the perpendicular direction, which can be calculated as

$$x = \frac{h(P_U+P_D)}{P_F-P_B}.$$

Therefore, the entire routing path length can be estimated as

$$h\sqrt{1+\left(\frac{P_U+P_D}{P_F-P_B}\right)^2}, \tag{7}$$

and the total number of routing hops can be estimated by

$$\frac{h\sqrt{1+\left(\frac{P_U+P_D}{P_F-P_B}\right)^2}}{P_F-P_B}.$$

■

According to Section IV-A1, in our case G_1, G_2, G_3 and G_4 correspond the sections F, B, U and D, respectively. Therefore, we have $P_F = P_1, P_U = P_2, P_D = P_3, P_B = P_4$. Based on Theorem 1, the total number of routing hops can be estimated according to the following corollary.

Corollary 1. *Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then for a given EBC parameter α and the hop distance h for α = 0, the number of routing hops can be estimated from the following equation:*

$$\frac{h\sqrt{1+\left(\frac{P_2+P_3}{P_1-P_4}\right)^2}}{P_1-P_4}. \tag{8}$$

TABLE I

ROUTING HOPS FOR DIFFERENT EBC PARAMETERS ($\mu' = 200$, $\sigma' = 50\sqrt{2}$)

EBC parameter	Average hops in simulations	Estimated CASER hops
0	10	10
0.1	10.26	10.05
0.2	10.38	10.09
0.3	10.63	10.18
0.4	11.02	10.34
0.5	11.15	10.64

Our simulation results conducted using OPNET network performance analysis tool demonstrate that Corollary 1 provides a very good approximation on the actual number of routing hops, as shown in Table I.

B. Secure Routing Strategy

In the previous section, we only described the shortest path routing grid selection strategy. However, in CASER protocol, we can support other routing strategies. In this section, we propose a routing strategy that can provide routing path unpredictability and security. The routing protocol contains two options for message forwarding: one is a deterministic shortest path routing grid selection algorithm, and the other is a secure routing grid selection algorithm through random walking.

In the deterministic routing approach, the next hop grid is selected from $\mathcal{N}_A^\alpha$ based on the relative locations of the grids. The grid that is closest to the sink node is selected for message forwarding. In the secure routing case, the next hop grid is randomly selected from $\mathcal{N}_A^\alpha$ for message forwarding. The distribution of these two algorithms is controlled by a *security level* called $\beta, \beta \in [0, 1]$, carried in each message.

When a node needs to forward a message, the node first selects a random number $\gamma \in [0, 1]$. If $\gamma > \beta$, then the node selects the next hop grid based on the shortest routing algorithm; otherwise, the next hop grid is selected using random walking. The security level β is an adjustable parameter. A smaller β results in a shorter routing path and is more energy efficient in message forwarding. On the other hand, a larger β provides more routing diversity and security.

C. CASER Algorithm

Based on the previous description, the CASER algorithm can be described in Algorithm 2. While providing routing path security, security routing will add extra routing overhead due to an extended routing path.

Algorithm 2 Node A finds the next hop routing grid based on the given parameters $\alpha, \beta \in [0, 1]$

```
Compute the average remaining energy of the adjacent
  neighboring grids: $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.
Determine the candidate grids for the next routing hop:
  $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \ge \alpha\mathcal{E}_a(A)\}$.
Select a random number $\gamma \in [0, 1]$.
if $\gamma > \beta$ then
    Send the message to the grid in the $\mathcal{N}_A^\alpha$ that is closest
    to the sink node based on its relative location.
else
    Route the message to a randomly selected grid in the set
    $\mathcal{N}_A^\alpha$.
end if
```

When β increases, the probability for the next hop grid to be selected through random walking also increases. Accordingly, the routing path becomes more random. In particular, when $\beta = 1$, then random walking becomes the only routing strategy for the next hop grid to be selected. The existing research [19], [20] has demonstrated that the message may never be delivered from the source node to the destination node in this case.

When $\beta < 1$, since CASER mixes random walking with deterministic shortest path routing, the deterministic shortest path routing guarantees that the messages are sent from the source node to the sink node. However, the routing path becomes more dynamic and unpredictable. In this way, it is more difficult for the adversary to capture the message or to jam the traffic. Therefore, the delivery ratio can be increased in a hostile environment. While providing routing security, routing hop distance increases with the security level β. Corollary 2 provides a quantitative estimation of the routing hops in this scenario.

TABLE II
ROUTING HOPS FOR VARIOUS SECURITY PARAMETERS. THE SIMULATION WAS PERFORMED USING OPNET.

Security parameter β	Average hops in simulations	Estimated CASER hops
0	10.00	10.00
0.125	11.97	11.46
0.25	14.51	13.52
0.375	17.98	16.70
0.5	23.34	22.36

Corollary 2. *Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then the average number of routing hops for a message to be transmitted from the source to the sink nodes can be estimated as follows:*

$$\frac{h\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2}}{1-\beta}, \tag{9}$$

where h is the required number of hops when the security level $\beta = 0$ (i.e., when no security is enforced).

Proof: For a security level β, the probability that the message is routed forward using the deterministic shortest path routing strategy is $1 - \beta$. For probability β, the message is forwarded using random walking. At each source, similar to Theorem 1, we can divide the entire domain into four $\frac{\pi}{2}$ sections, correspond to F, U, D, B with probability $P_F = 1 - \frac{3\beta}{4}, P_U = P_D = P_B = \frac{\beta}{4}$. The rest part of the proof is straight according to Theorem 1. ■

Table II compares the average number of routing hops between simulation results and the estimation based on Corollary 2 for various security parameters .

Remark 1. *Corollary 1 and Corollary 2 are derived based on the assumption that the sensor nodes are randomly deployed. However, in our case, the remaining energy levels for the sensor nodes decrease exponentially when message are being transmitted based on distance between the sensor nodes and the sink node. Therefore, the actual number of routing hops should be slightly longer than this estimation.*

V. DETERMINE SECURITY LEVEL BASED ON COST FACTOR

Based on Corollary 2, for a given routing budget, we can also find the maximum routing security level. This result is given in the following theorem.

Theorem 2. *Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then for a given routing cost factor f, the optimal security level can be estimated from the following quartic equation:*

$$4fx^4 - 5x^2 + 2x - 1 = 0, \tag{10}$$

where $x = 1 - \beta$.

Proof: According to Corollary 2, we have

$$\frac{\sqrt{1 + \left(\frac{\beta}{2(1-\beta)}\right)^2}}{1-\beta} = f.$$

Multiply both sides with $1 - \beta$, we have

$$\sqrt{1 + \left(\frac{\beta}{2(1-\beta)}\right)^2} = f(1-\beta).$$

Square of both sides, we get

$$1 + \left(\frac{\beta}{2(1-\beta)}\right)^2 = f^2(1-\beta)^2.$$

Equivalently, we have

$$4(1-\beta)^2 + \beta^2 = 4f^2(1-\beta)^4.$$

Let $1 - \beta = x$, we can derive

$$\beta^2 = (1-x)^2 = x^2 - 2x + 1,$$

reorganize the above equation, we get

$$4f^2x^4 - 5x^2 + 2x - 1 = 0. \tag{11}$$

■

Equation (11) can be solved using Ferrari's method [23] following Algorithm 3 to recover $s = 1 - \beta$. The security level β can be recovered as: $\beta = 1 - s$.

Algorithm 3 Solve equation $4f^2x^4 - 5x^2 + 2x - 1 = 0$.

```
$a \leftarrow 4f^2; c \leftarrow -5; d \leftarrow 2; e \leftarrow -1;$
$A \leftarrow \frac{c}{a}; B \leftarrow \frac{d}{a}; C \leftarrow \frac{e}{a};$
$p \leftarrow -\frac{1}{12}A^2 - C; q \leftarrow -\frac{A^3}{108} + \frac{AC}{3} - \frac{B^2}{8};$
$r \leftarrow -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}};$
$u \leftarrow \sqrt[3]{r};$
$y \leftarrow -\frac{5}{6}A + u - \frac{p}{3u}; w \leftarrow \sqrt{A + 2y};$
$s \leftarrow \frac{-w + \sqrt{-3A - 2y + 2B/w}}{2}.$
```

Example 1. *Suppose we want to deliver a message with cost factor $f = 1.5$. To find the maximum routing security level, we need to find the security parameter β. We can compute $s = 1 - \beta$ as follows:*

1: $a \leftarrow 9; c \leftarrow -5; d \leftarrow 2; e \leftarrow -1;$
2: $A \leftarrow -0.556; B \leftarrow 0.222; C \leftarrow -0.111$*;*
3: $p \leftarrow 0.0854; q \leftarrow 0.016;$
4: $r \leftarrow 0.001$*;*
5: $u \leftarrow 0.110$*;*
6: $y \leftarrow 0.314; w \leftarrow 0.270$*;*
7: $s \leftarrow 0.684.$

Therefore, we have $\beta = 1 - s = 0.316$, which means 31.6% of the routing strategies should be based on random walking for message forwarding.

VI. Security Analysis

In CASER, the next hop grid is selected based on one of the two routing strategies: shortest path routing or random walking. The selection of these two routing strategies is probabilistically controlled by the security level β. The security level of each message can be determined by the message source according to the message priority or delivery preference. As β increases, the routing path becomes more random, unpredictable, robust to hostile detection, interception and interference attacks.

While random walking can provide good routing path unpredictability, it has poor routing performance [19], [20], [22]. CASER provides an excellent balance between routing security and efficiency.

A. Quantitative Security Analysis of CASER

In [1], we introduced criteria to quantitatively measure source-location privacy for WSNs.

Definition 1 ([1] Source-location Disclosure Index (SDI))**.** SDI *measures, from an information entropy point of view, the amount of source-location information that one message can leak to the adversaries.*

For a routing scheme, to achieve good source-location privacy, *SDI* value for the scheme should be as close to zero possible.

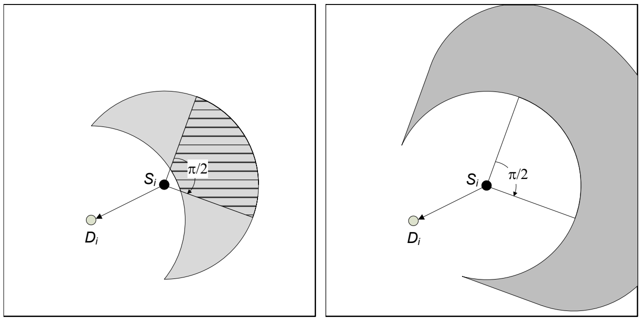
Definition 2 ([1] Source-location Space Index (SSI))**.** SSI *is defined as the set of possible network nodes, or area of the possible network domain, that a message can be transmitted from.*

For a source-location privacy scheme, *SSI* should be as large as possible so that the complexity for an adversary to perform an exhaustive search of the message source is maximized.

Definition 3 ([1] Normalized Source-location Space Index (NSSI))**.** NSSI *is defined as the ratio of the* SSI *area over the total area of the network domain. Therefore, $NSSI \in [0, 1]$, and we always have $NSSI = 1 - \delta$ for some $\delta \in [0, 1]$. The δ is called the local degree.*

Based on these criteria, we can evaluate security of the CASER routing protocol.

Theorem 3. *Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then the CASER routing protocol*



(a) Random walking (b) Deterministic routing

Fig. 2. Routing source traceback analysis.

can achieve perfect source node location information protection when $\beta > 0$, that is

$$SDI \simeq 0.$$

Proof: First, in CASER, according to our assumption, a dynamic ID is used for each message, which prevents the adversary from linking multiple messages from the same source or linking the message to the source direction using correlation based techniques.

Second, for $\beta > 0$, due to probabilistic distribution of random walking and deterministic routing, at each intermediate node, neither the original packet source direction, nor the hop distance can be determined through routing traceback analysis. In fact, the adversary is infeasible to determine the previous hop source node through routing traceback analysis. Moreover, the probability for the adversary to receive multiple messages from the same source node continuously is negligible for large sensor networks. Therefore, we have

$$SDI \simeq 0.$$

■

Theorem 4. *Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then the source location that can be provided by the CASER routing protocol is probabilistically proportional to the distribution of the random walking. That is*

$$NSSI \simeq 1.$$

Proof: When an adversary intercepts a message m while the message is being transmitted from node A to node B, there are two possible scenarios: (i) the message is transmitted using random walking, or (ii) the message is transmitted using deterministic routing.

For scenario (i), suppose message m is transmitted from S_i to D_i, the previous source node is located in shaded area, as shown in Fig. 2(a), based on the routing scheme and routing hop distance, where the angle of the shaded circular sector with horizontal lines is $\frac{\pi}{2}$ and symmetric to the S_iD_i.

Since each node routes the message forward with probability $1-\beta$ using deterministic routing and with probability β using random walking. It can be derived that the probability for the immediate previous hop node to be located in the shaded sector is $1-\beta+\frac{\beta}{4} = 1-\frac{3}{4}\beta$, and to be located in the rest of the shaded area is $\frac{3}{4}\beta$.

The probability advantage for the immediate previous hop node to be in the shared sector area with horizontal lines is,

$$1-\frac{3}{4}\beta-\frac{1}{4} = \frac{3}{4}(1-\beta).$$

However, when the traceback analysis continues, we will not be able to get any probability advantage for the next previous hop routing source node, except that the node will be located in the shaded area, given in Fig. 2(b), based on the hop distance.

Since the hop distance between the actual source node and the current intercepted node is unknown, this makes it impossible for the actual source node to be located in the sensor domain, with an negligible exception of a small area around the node D_i. Therefore, we have

$$NSSI \simeq 1.$$

■

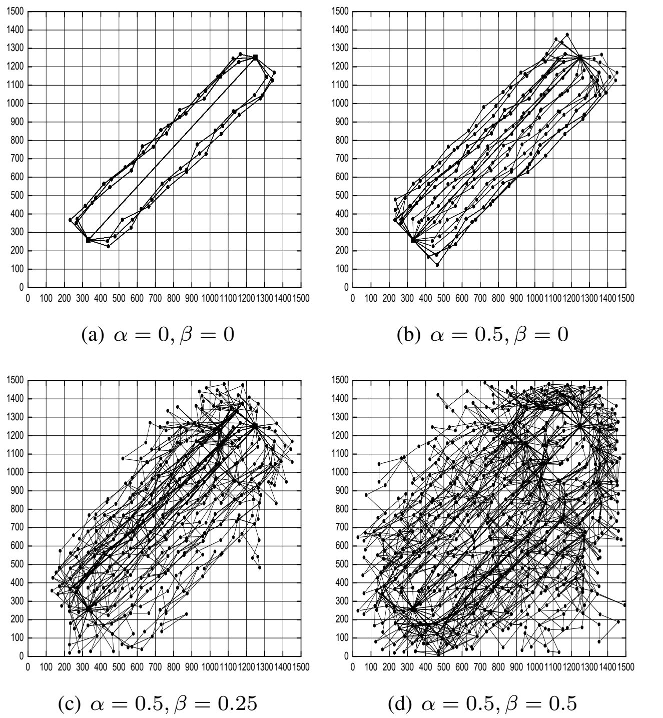
Remark 2. *From the proof of Theorem 4, we can see that the adversary can only get probability advantage $\frac{3}{4}(1-\beta)$ of one hop source node. In particular, when $\beta = 1$, that is the case of random walking, the adversary is unable to get any probability advantage.*

B. Dynamic Routing and Jamming Attacks

For security level β, the distribution between random walking and the shortest path routing for the next routing hop is β and $1-\beta$. β can vary for each message from the same source. In this way, the routing path becomes dynamic and unpredictable. In addition, when an adversary receives a message, he is, at most based on our assumption, able to trace back to the immediate source node that the message was transmitted. Since the message can be sent to the previous node by either of the routing strategies, it is infeasible for the adversary to determine the routing strategy and find out the previous nodes in the routing path.

Fig. 3 gives the routing path distribution for four different security levels using OPNET. The messages are transmitted from a single source located at $(332, 259)$ to the fixed sink node located at $(1250, 1250)$. The source node and the destination node are 10 hops away in direct distance. In the figures, each line represents a routing path used by at least one message. This figure demonstrates that the routing path distribution width increases with the energy balance control α and the security parameter β.

In fact, if we assume that the minimum number of hops between the source node and the sink node is h for $\beta = 0$, then for $\beta > 0$, the total number of random walking is about $\frac{h\beta}{1-\beta}$ hops. The routing path can be spread largely in the area of width $\frac{h\beta}{1-\beta}$ centered around the path for security level $\beta = 0$. Therefore, for a larger security level, more effort is required to intercept a message since it triggers more random walking, which will create a wider routing path distribution



(a) $\alpha = 0, \beta = 0$

(b) $\alpha = 0.5, \beta = 0$

(c) $\alpha = 0.5, \beta = 0.25$

(d) $\alpha = 0.5, \beta = 0.5$

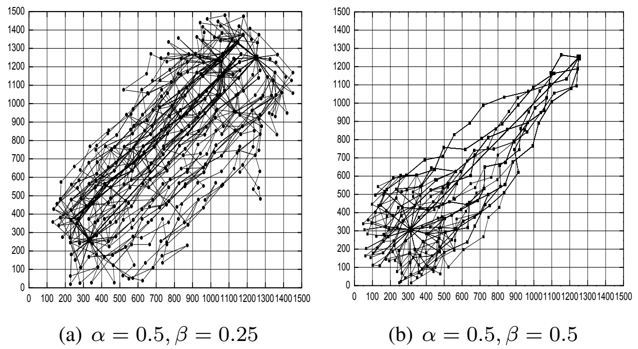
Fig. 3. Routing path distribution statistics for various energy balance control α and security parameters β. In all simulations, the target area is 1500×1500. The source node is located at $(332, 259)$ and sink is located at $(1250, 1250)$.

and a higher routing robustness under hostile attacks. As a result, the adversary has to monitor a larger area in order to intercept/jam a message. As an example, when $\beta = 0.5$, the width of the routing path is about the same as the length of the routing path, as shown in Fig. 3(d).

Jamming attacks have been extensively studied [24], [25]. The main idea is that the jammers try to interfere with normal communications between the legitimate communication parties in the link layer and/or physical layer. However, a jammer can perform attacks only when the jammer is on the message forwarding path. As discussed in [25], dynamic routing is an effective method to minimize the probability of jamming. The CASER routing algorithm distribute the routing paths in a large area based on our above analysis due to the random and independent routing selection strategy in each forwarding node. This makes the likelihood for multiple messages to be routed to the sink node through the same routing path very low even for the smart jammers that have knowledge of the routing algorithm.

C. Energy Level and Compromised Node Detection

Since we assume that each node has knowledge of energy levels of its adjacent neighboring grids, each sensor node can update the energy levels based on the detected energy usage. The actual energy is updated periodically. For WSNs with non-replenishable energy resources, the energy level is a monotonically decreasing function. The updated energy level should never be higher than the predicated energy level since the predicted energy level is calculated based on only the actually detected usage. If the updated energy level is higher than the predicted level, the node must have been compromised and should be excluded from its list of the adjacent neighboring grids.



(a) $\alpha = 0.5, \beta = 0.25$

(b) $\alpha = 0.5, \beta = 0.5$

Fig. 4. Routing path distribution statistics for energy balance control $\alpha = 0.5$ and security parameters $\beta = 0.25$ and RSIN in [20] with parameters: $d_{min} = 100, \rho = 3$.

We also compared the CASER algorithm with the RSIN algorithm in [20] on path distribution under the similar energy consumption. The results show that the CASER can achieve better and more uniform path distribution, as shown in Fig. 4. Our simulation results show that the average number of routing hops for the two schemes are 14.51 and 15.27, respectively.

In addition, for a node with a low energy level that is caused by excessive usage due to security attacks, according to our design, these nodes will be filtered out of the pool for active routing selection. Therefore, the CASER design can minimize the possibility for denial-of-service (DoS) attacks.

VII. Performance Evaluation and Simulation Results

In this section, we will analyze the routing performance of the proposed CASER protocol from four different areas: routing path length, energy balance, the number of messages that can be delivered and the delivery ratio under the same energy consumption. Our simulations were conducted in a targeted sensor area of size 1500×1500 meters divided into grids of 15×15.

A. Routing Efficiency and Delay

For routing efficiency, we conduct simulations of the proposed CASER protocol using OPNET to measure the average number of routing hops for four different security levels. We randomly deployed 1000 sensor nodes in the entire sensor domain. We also assume that the source node and destination node are 10 hops away in direct distance. The routing hops increase as the number of transmitted messages increase. The routing hops also increase with the security levels.

We performed simulations with different α and β values as shown in Tables I and II. In all cases, we derived consistent results showing that the average number of routing hops derived in this paper provides a very close approximation to the actual number of routing hops. As expected, when the energy level

TABLE III
DELAY RESULTS FOR VARIOUS SECURITY PARAMETER FROM SIMULATION

Security Parameter	0	0.125	0.25	0.375	0.5
Average Delay (Sec)	0.0148	0.0177	0.0214	0.0265	0.0344

goes down, the routing path spreads further wider for better energy balance.

We also provided simulation results on end-to-end transmission delay in Table III.

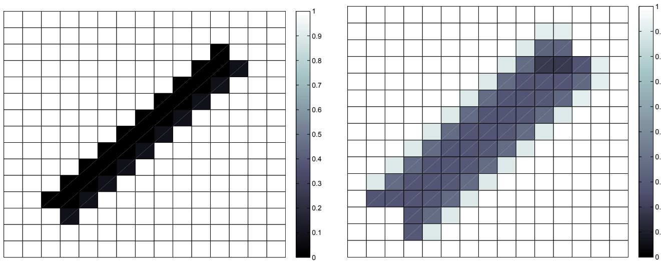
B. Energy Balance

The CASER algorithm is designed to balance the overall sensor network energy consumption in all grids by controlling energy spending from sensor nodes with low energy levels. In this way, we can extend the lifetime of the sensor networks. Through the EBC α, energy consumption from the sensor nodes with relatively lower energy levels can be regulated and controlled. Therefore, we can effectively prevent any major sections of the sensor domain from completely running out of energy and becoming unavailable.

In the CASER scheme, the parameter α can be adjusted to achieve the expected efficiency. As α increases, better energy balance can be achieved. Meanwhile, the average number of routing hops may also increase. Accordingly, the overall energy consumption may go up. In other words, though the energy control can balance the network energy levels, it may increase the number of routing hops and the overall energy consumption slightly. This is especially true when the sensor nodes have very unbalanced energy levels.

In our simulations, shown in Fig. 5, the message source is located at (332, 259) and the message destination is located at (1250, 1250). The source node and the destination node are 10 hops away in direct distance. There are three nodes in each grid, and each node is deployed with energy to transmit 70 messages. We show the remaining energy levels of the sensor nodes under two different α levels. The darker gray-scale level corresponds to a lower remaining level. Fig. 5(a), we set $\alpha = 0$ and there is only one source node. The energy consumption is concentrated around the shortest routing path and moves away only until energy runs out in that area. In Fig. 5(b), we set $\alpha = 0.5$, then the energy consumption is spread over a large area between this node and the sink. While maximizing the availability of the sensor nodes, or lifetime, this design can also guarantee a high message delivery ratio until the energy runs out for all of the available sensor nodes in the area.

We also conducted simulations to evaluate the energy consumption for dynamic sources in Fig. 6. We assume that the only sink node is located in the center of the sensor domain. There are three nodes in each grid, and each node is deployed with energy to transmit 70 messages. In this case, the energy consumption is highest for the node around the sink node. The consumption decreases based on the distance that the node is away from the sink node. In fact, the average energy consumption for the node with distance i to the sink node can be calculated as follows.



(a) $\alpha = 0$

(b) $\alpha = 0.5$

Fig. 5. Remaining energy distribution statistics after the source transmitted about 600 messages.

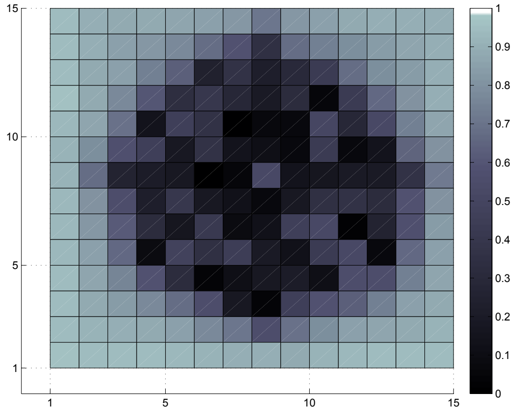


Fig. 6. The remaining energy levels of the sensor nodes in the sensor domain when the innermost grid almost runs out of the energy, where $\alpha = 0.5, \beta = 0.5$.

Theorem 5. *Assume that all sensor nodes transmit messages to the sink node at the same frequency, the initial energy level of each grid is equal, then the average energy consumption for the grid with distance i to the sink node is:*

$$\frac{n^2 + n + i - i^2}{2i}, \tag{12}$$

where n is the distance between the sink node and the outmost grid.

Proof: Since all messages will be sent to the sink node, the energy consumption for the grids with distance i to the sink node can be measured based on message forwarding for grids with distance larger than i and message transmission for grids with distance i. The number of grids with distance j to the sink node is $8j$. The total energy consumption of the grids with distance i to the sink can be calculated as $\sum_{j=i}^{n} 8j$. The average grid energy consumption is therefore:

$$\frac{\sum_{j=i}^{n} 8j}{8i} = \frac{n^2 + n + i - i^2}{2i}. \qquad \blacksquare$$

To investigate the energy consumption in the uniform energy deployment, we assume each sensor node has equal probability to generate packets and acts as a source node in Fig. 6 and Fig. 7.

In these simulations, the the sink node is located in the center of the target area located at (750, 750), which makes the target area symmetrical to show the energy consumption. Each node

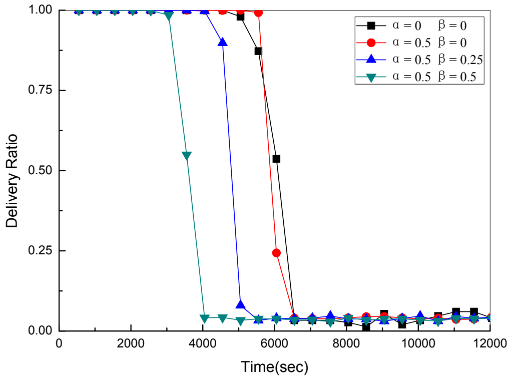


Fig. 7. Delivery ratio under different EBC α and security level β.

has the same probability to generate the packets. The maximum direct distance between the source node and sink is 7. Similar to the previous simulation, we assume there are three nodes in each grid, and each node is deployed with energy to transmit 70 messages.

Fig. 6 gives the remaining energy levels close to the sink node when the sensor nodes run out almost the entire energy, where $n = 7, \alpha = 0.5, \beta = 0.5$. The color evenness in each layer of the grids demonstrates the energy usage balance enforced through the EBC α.

In fact, according to equation (12), we can calculate the total number of messages that can be transmitted from the outmost grid when the innermost grid runs out of energy as $210/((n^2+n)/2) = 210/((7^2+7)/2) = 7.5$. In this case, the overall energy consumption is only $7.5 \times \sum_{i=1}^{n} 8j^2 = 8400$, when the sensor networks become unavailable. Recall that the overall energy units deployed are $210 \times ((2n+1)^2 - 1) = 47040$. Therefore, the energy consumption is only $8400/47040 = 5/28 \approx 17.86\%$ when the innermost grids run out of energy and become unavailable.

C. Delivery Ratio

One of the major differences between our proposed CASER routing protocol and the existing routing schemes is that we try to avoid having any sensor nodes run out of energy while the energy levels of other sensor nodes in that area are still high.

We implement this by enforcing a balanced energy consumption for all sensor nodes so that all sensor nodes will run out of energy at about the same time. This design guarantees a high message delivery ratio until energy runs out from all available sensor nodes at about the same time. Then the delivery ratio drops sharply. This has been confirmed through our simulations, shown in Fig. 7.

VIII. CASER Optimal Non-Uniform Energy Deployment

CASER is designed to balance the energy consumption of sensor nodes and thereby extends the lifetime of the sensor networks. However, as we have described in Section VII-B, the energy consumption is uneven in sensor networks. The energy consumption for the sensor nodes closer to the sink node is much higher than the nodes that are away from the sink node. In fact, the average energy consumption for the node with distance i to the sink node can be calculated according to equation (12). Therefore, the best that we can do is to balance the energy of the grids with the same radius to the sink node, as shown in Fig. 6.

In this section, we will explore the optimal, non-uniform initial energy deployment strategy that can maximize the lifetime of the sensor networks. Suppose the original energy distribution for each grid is the same, and we denote the energy level as u. We also assume that the largest distance between the sink node and the outmost grid is n, then the total energy unit is $u((2n+1)^2 - 1)$.

A. Node Energy Deployment

For the optimal energy deployment, the energy allocation of the grids should be proportional to the energy usage. We still assume that the sink node is in the center of the sensor domain. All sensor nodes transmit messages at the same frequency. The distance between the outmost grid and the sink node is n according to equation (12), the energy allocation for the grids with hop distance i to the sink node should be:

$$\frac{n^2+n+i-i^2}{2i}v,$$

where v is the basic energy unit for energy deployment. Accordingly, from the outmost to the innermost, the energy assignment should be:

$$v, \frac{2n-1}{n-1}v, \frac{3(n-1)}{n-2}v, \cdots, \frac{(n+2)(n-1)}{4}v, \frac{(n+1)n}{2}v.$$

The total energy units should be:

$$v\left(\frac{8}{3}n^3 + 4n^2 + \frac{4}{3}n\right).$$

To maintain the same amount of energy, we let:

$$u((2n+1)^2 - 1) = v\left(\frac{8}{3}n^3 + 4n^2 + \frac{4}{3}n\right).$$

Then we have:

$$v = \frac{3n}{(2n+1)(n+1)}u. \tag{13}$$

Example 2. *We still assume that $n = 7$, and each grid has $u = 210$ energy units originally. According to equation (13), we can derive that:*

$$v = \frac{3u}{2n+1}u = 42.$$

Therefore, the non-uniform energy deployment for all of the grids from the outmost to the innermost can be calculated as:

$$42, 91, 151, 231, 350, 567, 1176.$$

With this energy deployment, we maintained the same overall amount of energy deployment units, 47040, in the non-uniform energy deployment. However, under our assumption, the energy consumption should be 100% before the sensor network runs out of energy and dies. Recall that in the uniform energy deployment scenario, the sensor network dies when only about 17.86% of the energy is consumed. Therefore, under non-uniform deployment, the efficiency of a sensor network's energy usage can be roughly $100/17.86 = 5.6$ times compare to the uniform energy deployment. The efficiency can be measured by the total number of messages that can be delivered, or the lifetime of the sensor network under the same transmission frequency.

B. Routing in Non-Uniform Energy Deployment

Under the new energy deployment, we have to redefine the way we calculate the average remaining energy of the adjacent neighboring grids since otherwise, the messages will always be routed to the nodes that are closer to the sink node, at least initially. In this way, the number of possible nodes for the next hop can be greatly limited and security routing may become trivial.

For the non-uniform energy deployment case, the energy assignment is proportional to the energy consumption. In other words, the energy assignment is constant when divided by the energy consumption factor $\frac{n^2+n+i-i^2}{2i}$, where $i = 1, 2, \cdots, n$. Therefore, we can define the average remaining level as:

$$\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|} \sum_{i \in \mathcal{N}_A} \frac{\mathcal{E}r_i}{\frac{n^2+n+i-i^2}{2i}}. \tag{14}$$

Accordingly, we have the updated Algorithm 4.

Algorithm 4 Node A finds the next hop routing grid based on the given parameters $\alpha, \beta \in [0, 1]$

```
Compute the average remaining energy of the adjacent neighboring grids: $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|} \sum_{i \in \mathcal{N}_A} \frac{\mathcal{E}r_i}{\frac{n^2+n+i-i^2}{2i}}$.
Determine the candidate grids for the next routing hop: $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha \mathcal{E}_a(A)\}$.
Select a random number $\gamma \in [0, 1]$.
**if** $\gamma > \beta$ **then**
    Send the message to the grid in the $\mathcal{N}_A^\alpha$ that is closest to the sink node based on its relative location.
**else**
    Route the message to a randomly selected grid in the set $\mathcal{N}_A^\alpha$.
**end if**
```

C. Simulation Results

We conducted simulations using OPNET to compare the message delivery ratio of uniform energy deployment (noED) and non-uniform energy deployment (ED) for different α values when $\beta = 0$. The simulation settings are similar to Fig. 6. However, each node is deployed with a different energy level according to Algorithm 4. From the simulation results in Fig. 8(a), we can see that the delivery ratio increases with α. Comparing to uniform energy deployment, the delivery ratio for non-uniform energy deployment is much higher than the uniform energy deployment with the same α.

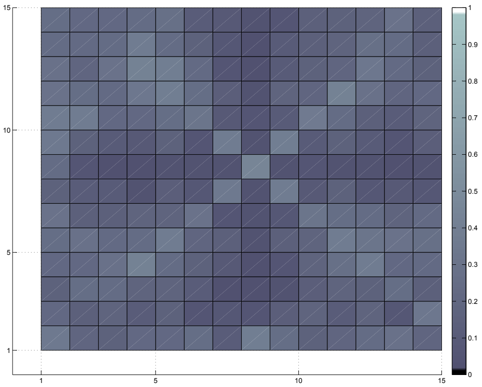


Fig. 9. A snapshot of energy distribution when the remaining energy is about 10% in the sensor nodes, where $\alpha = 0.5, \beta = 0.5$.

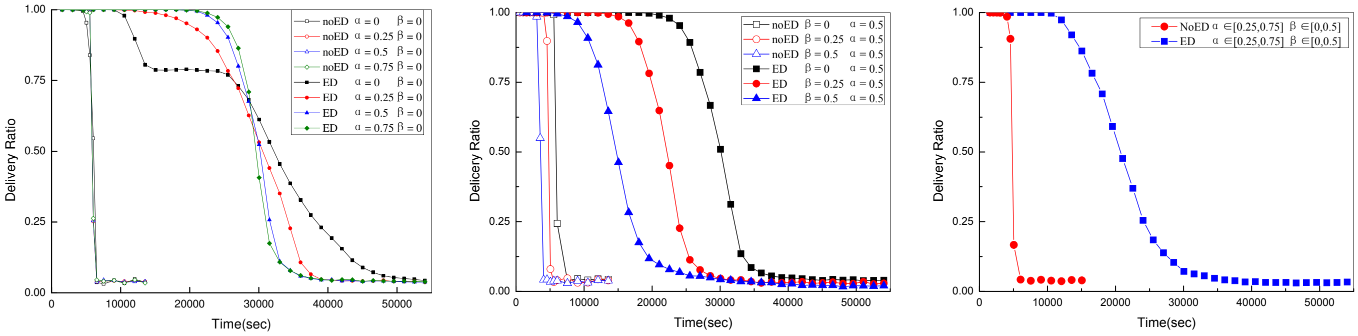
We also compared the total number of messages that can be delivered in the two scenarios. Our statistics are based on the message delivery ratio that is 95% or above. In uniform energy deployment, when $\alpha = 0$, the number of messages that can be delivered is 1510. When $\alpha = 0.25$, the number of messages that can be delivered increases to 1624. The increase is 7.55%. We found that when we further increase α, the number of messages that can be transmitted increases slightly. At this point, all the nodes around the sink have run out of energy and no more messages can be transmitted.

For the non-uniform deployment, when $\alpha = 0, 0.25, 0.5$ and 0.75, the ratio of the number of messages that can be delivered between non-uniform and uniform is 2.37, 4.2, 5.16 and 5.38, respectively. The simulation results demonstrate that the proposed CASER and non-uniform energy deployment can significantly increase the delivery ratio and the lifetime of the WSN.

When $\beta \neq 0$, from Fig. 8(b) we can see that the message delivery ratio drops as β increases. This is because the overall energy consumption increases as the required security level increases. We also found that under the proposed CASER protocol, non-uniform energy deployment can increase the energy efficiency and network lifetime even when security is required in WSNs.

Fig. 8(c) provides the message delivery ratio in a more realistic scenario. Since the different messages may have different importance, we select both security parameters and energy balance levels randomly for non-uniform and uniform energy deployment in this simulation. The results demonstrate that non-uniform energy deployment can achieve a much higher delivery ratio while extending the lifetime of the WSN.

Fig. 9 shows the energy consumption of the WSN for non-uniform energy deployment. Comparing the two results, we conclude that CASER can achieve excellent energy balance. All sensor nodes run out of energy at about the same time, while in uniform energy deployment, the energy consumption is very unbalanced, as shown in Fig. 6.



(a) (b) (c)

Fig. 8. Message delivery ratio: (a) $\beta = 0$ and varying α, (b) $\alpha = 0.5$ and varying β, (c) varying α and β, where $\alpha \in [0.25, 0.75], \beta \in [0, 0.5]$

IX. Conclusions

In this paper, we presented a secure and efficient Cost-Aware SEcure Routing (CASER) protocol for WSNs to balance the energy consumption and increase network lifetime. CASER has the flexibility to support multiple routing strategies in message forwarding to extend the lifetime while increasing routing security. Both theoretical analysis and simulation results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. Our analysis and simulation results show that we can increase the lifetime and the number of messages that can be delivered under the non-uniform energy deployment by more than four times.

References

[1] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, accepted, to appear.

[2] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in *IEEE INFOCOM 2012 Mini-Conference*, Orlando, Florida, USA., March 25-30, 2012 2012.

[3] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *MobiCom'2000*, New York, NY, USA, 2000, pp. 243 – 254.

[4] J. Li, J. Jannotti, D. S. J. D. C. David, R. Karger, and R. Morris, "A scalable location service fo geographic ad hoc routing," in *MobiCom'2000*. ACM, 2000, pp. 120 – 130.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in *the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks," *UCLA Computer Science Department Technical Report, UCLA-CSD*, May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor localization for very small devices," Computer science department, University of Southern California, Tech. Rep. Technical report00-729, April 2000.

[8] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the Seventh ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, July 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in adhoc wireless networks," in *3rd Int. Workshopon Discrete Algorithms and methods for mobile computing and communications*, 1999, pp. 48–55.

[10] ——, "Routing with guaranteed delivery in ad hoc wireless networks," in *the 3rd ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL M 99)*, Seattle, WA, August 1999, pp. 48–55.

[11] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in *Proc. IEEE INFOCOM*, vol. 3, March 2004, pp. 1705 –1716 vol.3.

[12] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 4, pp. 582–595, April 2010.

[13] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*, vol. 1, 17-21 March 2002, pp. 350 – 355 vol.1.

[14] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," *Networking, IEEE/ACM Transactions on*, vol. 12, no. 4, pp. 609–619, August 2004.

[15] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.

[16] F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 7, pp. 2258–2267, July 2010.

[17] C.-C. Hung, K.-J. Lin, C.-C. Hsu, C.-F. Chou, and C.-J. Tu, "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in *Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on*, Aug. 2010, pp. 1–6.

[18] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *SASN*. ACM, 2004, pp. 88–93.

[19] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *Proceedings of IEEE SECON 2009*, Rome, Italy., June 22-26, 2009.

[20] ——, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proceedings of IEEE INFOCOM 2010*, San Diego, USA., March 15-19, 2010.

[21] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, April 2008, pp. 51 – 55.

[22] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," *ICDCS*, pp. 599–608, June 2005.

[23] WikipediA, "Quartic function," http://en.wikipedia.org/wiki/Quartic_function.

[24] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[25] A. Pathan, H.-W. Lee, and C. seon Hong, "Security in wireless sensor networks: issues and challenges," in *The 8th International Conference on Advanced Communication Technology (ICACT)*, vol. 2, 2006, pp. 6 pp.–1048.