**INTRODUCTION**

**1.1 Background**

A wireless sensor network (WSN) is a [computer network](http://en.wikipedia.org/wiki/Computer_network) consisting of spatially distributed [autonomous](http://en.wikipedia.org/wiki/Autonomous) devices using [sensors](http://en.wikipedia.org/wiki/Sensor) to cooperatively monitor physical or environmental conditions, such as [temperature](http://en.wikipedia.org/wiki/Temperature), [sound](http://en.wikipedia.org/wiki/Sound), [vibration](http://en.wikipedia.org/wiki/Oscillation), [pressure](http://en.wikipedia.org/wiki/Pressure), motion or pollutants, at different locations.[[1]](http://en.wikipedia.org/wiki/Sensor_network#_note-romer2004) The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.[[1]](http://en.wikipedia.org/wiki/Sensor_network#_note-romer2004)

In addition to one or more sensors, each node in a sensor network is typically equipped with a [radio](http://en.wikipedia.org/wiki/Radio) [transceiver](http://en.wikipedia.org/wiki/Transceiver) or other wireless communications device, a small [microcontroller](http://en.wikipedia.org/wiki/Microcontroller), and an energy source, usually a [battery](http://en.wikipedia.org/wiki/Battery_%28electricity%29). The size a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust.[[1]](http://en.wikipedia.org/wiki/Sensor_network#_note-romer2004) The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes.[[1]](http://en.wikipedia.org/wiki/Sensor_network#_note-romer2004) Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.[[1]](http://en.wikipedia.org/wiki/Sensor_network#_note-romer2004)

Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure 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 trace- back 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 pro-posed 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 trace back attacks and malicious trafﬁc jamming attacks in WSNs.

**1.2 Aims and Objectives**

The main aim and object of this project is that

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 (ED).

3. We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control (EBC) and security requirements.

4. We quantitatively analyze security of the proposed routing algorithm.

5. We provide an optimal non-uniform energy deployment (noED) 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.

**1.3 Motivation**

The main motivation of this project is that

1. To maximize the sensor network lifetime, we ensure that the energy consumption of all sensor grids are balanced.

2. To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping when an alternative routing path exists.

3. The adversaries should not be able to get the source location information by analyzing the trafﬁc pattern.

4. 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.

5. 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.

6. 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.

**1.4 Proposed Work**

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

**LITERATURE SURVEY**

**2.1 Literature Survey**

**1**. **S. Mini and Siba Udgade in 2013 proposed** Wireless Sensor Networks (WSNs) are important for many applications such as military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, environment monitoring, and building and structural monitoring. Network lifetime (defined as the time instant from which the network starts functioning to the time instant where the desired coverage criterion is not satisfied) is a crucial factor that determines the efficiency of a wireless sensor network. Energy usage should be curbed to achieve enhanced lifetime. This is because sensor nodes are battery powered and cannot be easily recharged or replaced.

**2**. **Junbin LIANG, 2Ming LIU, 2 Xiaoyan KUI** 29 January 2014 proposed Coverage problem is an important issue in wireless sensor networks, which has a great impact on the performance of wireless sensor networks. Given a sensor network, the coverage problem is to determine how well the sensing field is monitored or tracked by sensors. In this paper, we classify the coverage problem into three categories: area coverage, target coverage, and barrier coverage, give detailed description of different algorithms belong to these three categories. Moreover, we specify the advantages and disadvantages of the existing classic algorithms, which can give a useful direction in this area.

**3**. **Qi Jing ,Athanasios V. Vasilakos,Jiafu Wan** suggested Internet of Things (IoT) is playing a more and more important role after its showing up, it covers from traditional equipment to general household objects such as WSNs and RFID. With the great potential of IoT, there come all kinds of challenges. This paper focuses on the security problems among all other challenges. As IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT. And as IoT contains three layers: perception layer, transportation layer and application layer, this paper will analyze the security problems of each layer separately and try to find new problems and solutions. This paper also analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them. In the end, this paper compares security issues between IoT and traditional network, and discusses opening security issues of IoT.

**4**. **Abhishekh jain and kamal kant** in 2012 suggested that Wireless Sensor Network (WSN) is a talented technology that shows great assurance for a variety of ultramodern applications both for mass public and military. The appearance of sensor networks as one of the central technology trends in the coming decades has posed several exclusive challenges to researchers. The key research spotlight has been on making sensor networks sufficient and helpful. This paper analyzes security requirements in wireless sensor networks and summarizes key issues, attacks and threats that should be solved for achieving the ad hoc security. We also present some secure solutions for achieving the security in wireless sensor networks.

**5**. **Nan Yao, Shaoping Wang, Yaoxing Shang\*, Jian Shi** ―Reliability of Wireless Sensor Network: Hotspot and Critical Challenges‖ Science and Technology on Aero craft Control Laboratory, School of Automation Science and Electrical Engineering Beihang University ©2012 IEEE

**6.** **E.Ilker Oymam and Cem Ersoy**, “Effect Of Overhead Energy To The Lifetime In WSN”. The paper presents an evaluates the use of multi-hop communication link and compares the amount of energy gained acquired by correct routing energy calculation. The researchers have analyzed the effects of neglecting the overhead energy deception and routing decisions.

**7**. **Bara’a A.Attea and Enan A.Khalil** “A New Evolutionary Based Routing Protocol For Clustered Heterogeneous Wireless Sensor Networks” volume 12, Issue 7, July 2012. This paper propose the undesirable behavior of the EA when dealing with clustered routing problem in WSN by formulating a new fitness function that incorporates two clustering aspects, viz. cohesion and separation error.

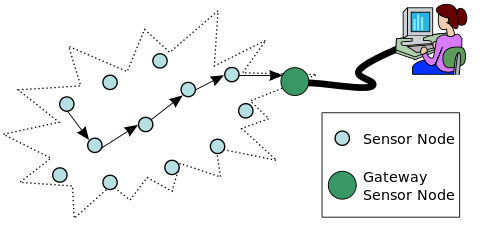
**8**. Y. Li, J. Li, J. Ren, and J. Wu, “Providing hop-by-hop authentication and source privacy in wireless sensor networks,” in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

**PROPOSED WORKS**

**3.1 Architecture of Wireless Sensor Network**

WSNs has emerged as an important technology for monitoring physical environment .WSNs consist of large number of sensor nodes which are small in size, inexpensive and battery powered. These WSNs can be used in various applications such as Military surveillance, environment monitoring, border protection, health care monitoring, weather monitoring. These applications require data without delay and energy consumed by them should be small. WSNs are deployed in harsh environment. Since it is not possible to replace or charge battery of sensor nodes, So it is desirable to design communication protocols such that energy source is used effectively and the delay in the network in minimum. Sensor nodes senses the environment, gathers the data from its surrounding(computation) and communicates it to the base station(BS).Out of the three tasks communication takes large amount of battery power of a sensor node, so the major concern is the communication task. We have to minimize the

Communication cost in order to save battery power. Wireless sensor networks [1] consists of a thousands of sensor nodes which are deployed randomly environment or space. In sensor network there is a BS(base 1station) which is located far away from the sensor field. Sensor nodes send the sensed data to the BS. For sending the sensed data to BS directly a lot of energy is consumed .So it is desirable to develop some protocols to minimized this communication cost. Energy conservation and maximization of network lifetime are the key challenges in the design and implementation of WSNs.



**Figure No: 3.1. Wireless Sensor Network**

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

**3.2 CASER Routing**

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 routing 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. In this project, 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

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.

CASER

Random walk Routing

Deterministic Routing

Use Random Selection Path

Use Shortest Path

Send Data Through Head Node

Send Data Through Head Node

**Figure No: 3.2. Architecture of CASER**

**3.3 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 NA and the remaining energy of grid i as €ri, i € NA. With this information, the node A can compute the average remaining energy of the grids in NA as €a(A)=

In the multi-hop routing protocol, node A selects its next hop grid only from the set NA 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 α € [0,1]& to enforce the degree of the energy balance control. We define the candidate set for the next hop node as ⃓ €ri based on the EBC a. It can be easily seen that a larger a corresponds to a better EBC. It is also clear that increasing of a may also increase the routing length. However, it can effectively control energy consumption from the nodes with energy levels lower than.

We summarize the CASER routing protocol in Algorithm 1. It should be pointed out that the EBC parameter a can be configured in the message level, or in the node level based on the application scenario and the preference. When a 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 shrinks as a increases. In other words, as α increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since is defined as

the average energy level of the nodes in NA, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from

**3.4 System Architecture**

**RESERCH METHODOLOGY**

**4.1 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.

**4.2 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 equipment’s, which means they would have some technical advantages over the sensor nodes. In this paper, the adversaries are assumed to have the following characteristics:

1. 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.

2. 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.

3. 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.

**4.3 Design Goals**

Our design goal can be summarized as follows:

1. To maximize the sensor network lifetime, we ensure that the energy consumption of all sensor grids are balanced.

2. To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping when an alternative routing path exists.

3. The adversaries should not be able to get the source location information by analyzing the traffic pattern.

4.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.

5. 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.

6. 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.

**4.4 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.

**4.5** **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 NA and the remaining energy of grid i as €ri, i € NA. With this information, the node A can compute the average remaining energy of the grids in NA as €a(A)=

In the multi-hop routing protocol, node A selects its next hop grid only from the set NA 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 α € [0,1]& to enforce the degree of the energy balance control. We define the candidate set for the next hop node as ⃓ €ri based on the EBC a. It can be easily seen that a larger a corresponds to a better EBC. It is also clear that increasing of a may also increase the routing length. However, it can effectively control energy consumption from the nodes with energy levels lower than.

We summarize the CASER routing protocol in Algorithm. It should be pointed out that the EBC parameter a can be configured in the message level, or in the node level based on the application scenario and the preference. When a 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 shrinks as a increases. In other words, as α increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since is defined as

the average energy level of the nodes in NA, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from

**Algorithm 1 Node A finds the next hop routing grid based on the EBC α**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1: Compute the average remaining energy of the adjacent neighboring grid

**2.** Determine the candidate grids for the next routing hop:

⃓ (A)}

3. Send the message to the grid in the that is closest to the sink node based on its relative location.

**4.6 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 sections,. 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 sections i (i=1, 2, 3, 4) corresponding to F(orward), U(pper), D(own) and B(ackward). The distance from the section Gi to the sink node is denoted as di. We also denote the remaining energy level of section i as 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 Ei can also be viewed as a random and independent and identically distributed (iid) variable.

Let f(dbe the probability distribution function (PDF) of Ei. 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:

1

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

Denote Pi as the probability that grid Gi is selected as the relay grid for message forwarding. Suppose d1 , then we have

Pi= 2

Where and  is the PDF of random variable Zi.

**4.7 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. 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 gird 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 Ei shall follow the normal distribution, that is where is the mean of the remaining energy level of each grid, si is the standard derivation of energy distribution.

|  |  |  |
| --- | --- | --- |
| EBC Parameter | Average hops in Simulation | 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 |

**Table no.4.1: Routing Hops for Different EBC Parameter**

**4.8 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 the extended routing path.

**Algorithm 2** Node a find the next hop routing grid based on the given parameter **α**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Compute the average remaining energy of the adjacent neighboring grid

2.Determine the candidate grids for the next routing hop:⃓ (A)}

3. Select random number **α**

4**. if** then send the message to the grid in the that is closest to the sink node based on its relative location.

**else**

Route the message to a randomly selected grid in the set

**end if**

When 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 , 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.

|  |  |  |
| --- | --- | --- |
| Security Parameter | Average hops in Simulation | 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 |
| 05 | 23.34 | 22.36 |

**Table no.4.2: Routing Hops for Various Security Parameter**

**4.9 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 b. The security level of each message can be determined by the message source according to the message priority or delivery preference.As b increases, the routing path becomes more random, unpredictable, robust to hostile detection, immune to

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.

**4.9.1 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 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 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 ;, and we always have NSSI =1- for some . The 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 can achieve perfect source node location information protection when b > 0, that is*

SDI

**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 > 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 h

SDI

**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 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 Si to Di, the previous source node is located in shaded area, as shown in Fig. 2a, based on the routing scheme and routing hop distance, where the angle of the shaded circular sector with horizontal lines is p2 and symmetric to the SiDi.

Since each node routes the message forward with probability 1 - using deterministic routing and with probability b using random walking. It can be derived that the probability for the immediate previous hop node to be located in the shaded sector is

and to be located in the rest of the shaded area is .

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

However, when the trackback 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. 2b, 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

NSSI 1

**4.9.2 Dynamic Routing and Jamming Attacks**

For security level , the distribution between random walking and the shortest path routing for the next routing hop is and 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 (1,250, 1,250). 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 a and the security parameter .

In fact, if we assume that the minimum number of routing hops between the source node and the sink node is h for then for > 0, the total number of random walking is about hops. The routing path can be spread largely in the area of width centered around the path for security level. 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 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 the width of the routing path is about the same as the length of the routing path.

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 distributes 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.

**PROJECT DESIGN**

**5 Performance Evaluations and Simulation**

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 1,500 1.500 meters divided into grids of 15 15.

**5.1 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 1,000 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 and values as shown in Tables 1 and 2. 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 goes down, the routing path spreads further wider for better energy balance.

**5.2 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 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 a can be adjusted to achieve the expected efficiency. As 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.

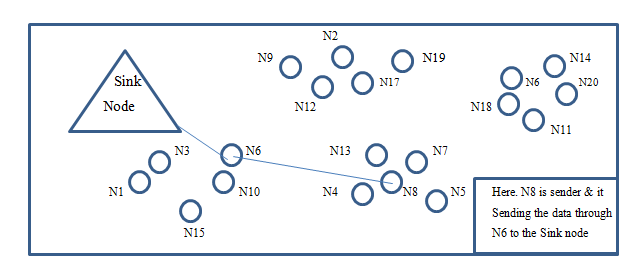
In our simulations, shown in Fig. 5, the message source is located at (332, 259) and the message destination is located at (1,250, 1,250). The source node and the destination node are 10 hops away in direct distance. There are three nodes in each grid, and each node is deployed with energy to transmit 70 messages. We show the remaining energy levels of the sensor nodes under two different a levels. The darker gray-scale level corresponds to a lower remaining level. Fig. 5a, we set 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. 5b, we set , 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.

**5.3 System Work**

In our theme, the network is equally divided into little grids. Each grid incorporates a relative location supported the grid data. The node in each grid with the best energy level is chosen as a result of the head node for message forwarding. To enhance, each node inside the grid will maintain its own attributes, as well as location data, remaining energy level of its grid, additional as a result of the attributes of its adjacent neighboring grids. The data maintained by each sensor node are updated intermittently.

System Design: during this paper, we tend to design a protocol i.e., CASER protocol. To use this protocol within the wireless sensor network at first we need to design the network. In figure1, we tend to consider that in our network we have additional range of sensors and one sink node. During this network are going to be partitioned as grids. In every grid equivalent sensor nodes are deployed. From the figure, we have four grids and in each grid have five sensor nodes. For complete network we have only single sink node.



**Figure no. 5.1: CASER Protocol Network Design**

It suggests that the sink node is simply destination for all sensor nodes. The data of the sink node is made public. For security functions, each message will be assigned a node identity equivalent to the situation the place this message is initiated. To prevent adversaries from raising the source location from the node identity, a dynamic id will be used. The content of every message also can be encrypted creating use of the key shared between the node/grid and therefore the sink node. We tend to additionally anticipate that each sensor node is attentive to its relative neighborhood among the sensor area and has competencies of its instant contiguous neighboring grids and their vigor levels of the grid. The understanding concerning the relative space of the sensor domain may even be broadcasted inside the network for routing data replace. Routing methods in CASER in this protocol, two types of methods are there: 1) Deterministic Routing Strategy and 2) Random Walk Routing Strategy.

**5.6.1. Deterministic Routing:**

Actually, the CASER protocol works supported two adjustable routing parameters such as follows: 1) Energy Balance control (EBC) and 2) random walk. In deterministic routing, we tend to use the EBC parameter. During this strategy we tend to implement the non-uniform energy readying strategy. During this strategy, initially all sensor nodes have constant energy and when some time they lose few quantity of energy. Remaining energies are we need to calculate initial. After that we tend to should choose the user grids.

****

**Figure no. 5.2: Deterministic Routing**

User grids suggest that based on calculated energy levels of sensor nodes; in each grid we have one high energy level node. We tend to choose that node to routing which node grid is referred to as a candidate grid. Supported elite candidate grids we tend to formulate a shortest path. Through that shortest path we tend to are causing the data. Finally, we are able to maintain the energy levels of the sensor nodes within the network. Like this, we are able to optimize the network lifetime with efficiency within the wireless sensor networks.

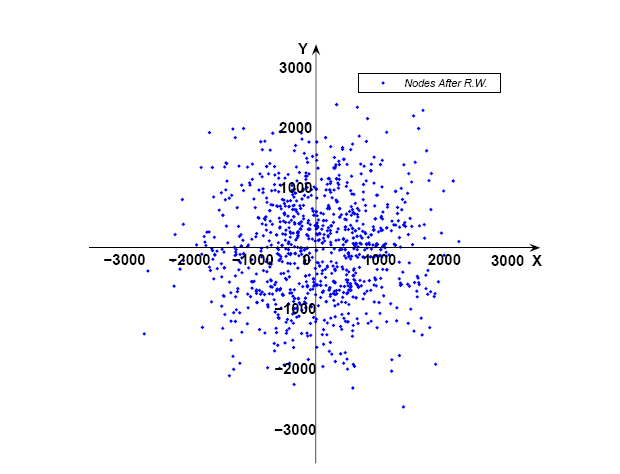
**5.6.2.Security in CASER Protocol**

In random walking parameter, CASER protocol sends the messages with secure. Once sender node sends the info to sink node, throughout transmission range of attacks are might occurred. So, during this protocol we tend to implemented Random walking strategy. To supply the safety we tend to choose the random walk routing strategy. It not only provides the safety to the node however additionally it managed the energy levels.

****

**Figure-5.3: Random Walking**

In random walk routing strategy, after we send the data through the shortest path it will not shows the sender node to protect the node details and corresponding data from the hackers. It simply hides the particular sender node details and it displays the closest node of the sender node as a sender node. By implementing likewise, there is no possibility to the aggressor to get the sender node details. If we tend to observe in figure3, the particular sender node is going to be set in shaded space and nearest node displayed as sender node. Here, supported node distance we are able to estimate that node is nearest to the sender node. Like this we are able to forward the messages from sender node to the sink node. During this paper, initial we tend to management the energy levels of the sensor nodes. After we are managed the sensor nodes energy levels within the network, then automatically, we tend to optimize the network lifespan. If network lifetime is increased, then we are able to increase the high message delivery ratio within the wireless sensor networks. Through the random walk strategy we can achieve the security side additionally at a time within the routing.



**Figure no 5.4 Node Distributions through random Walking**

**5.6.3 Project Code**

**RESULT OF PROPOSED METHOD**

**6.1 Snapshot**

**CONCLUSION & FUTURE SCOPE**

**7.1 Conclusion**

We conclude that in this project, we tend to present a secure and efficient Cost-Aware Secure Routing (CASER) protocol for wireless sensor networks. By using this protocol we will balance the energy consumption and reduce network lifetime improvement. Cost-Aware Secure Routing protocol has the flexibility to support multiple routing schemes in message forwarding to support network lifetime whereas improving routing security.

**7.2 Scope of Future work**

The Simulation results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. This 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.

Application of the proposed work will be

* Environmental monitoring
* Habitat monitoring
* Acoustic detection
* Seismic Detection
* Military surveillance
* Inventory tracking
* Medical monitoring
* Smart spaces
* Process Monitoring

**ADVANTAGES**

**8.1 Advantages**

1. Reduce the energy consumption

2. Provide the more secure for packet and also routing

3. Increase the message delivery ratio

4. Reduce the time delay

**8.2 Limitation**

1. More energy consumption

2. Increase the network collision

3. Reduce the packet delivery ratio

4. Cannot provide the full secure for packets

**HARDWARE AND SOFTWARE**

**Hardware Requirements**

1. System : Pentium IV 2.4 GHz.

2. Hard Disk : 40 GB.

3. Floppy Drive : 44 Mb.

4. Monitor : 15 VGA Colour.

5. Ram : 512 Mb.

**Software Requirements**

1. Operating system : Windows XP/7/LINUX.

2. Implementation : NS2

3. NS2 Version : 2.28

4. Front End : OTCL (Object Oriented Tool Command Language)

5. Tool : Cygwin (To simulate in Windows OS)

**REFERENCES**

[1] Y. Li, J. Ren, and J. Wu, “Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul.2012.

[2] Y. Li, J. Li, J. Ren, and J. Wu, “Providing hop-by-hop authentication and source privacy in wireless sensor networks,” in Proc.IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

[3] B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY, USA, 2000, pp. 243–254.

[4] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, “A scalable location service for geographic ad hoc routing,” in Proc.6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 120–130.

[5] Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad-hoc routing,” in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energyaware routing: A recursive data dissemination protocol for wireless sensor networks,” Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech. Rep., May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, “GPS-less low cost outdoor localization for very small devices,” Comput. Sci. Dept. Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00-729, Apr. 2000.

[8] A. Savvides, C.-C. Han, and M. B. Srivastava, “Dynamic finegrained localization in ad-hoc networks of sensors,” in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks,” in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun 1999, pp. 48–55.

[10] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks,” in Proc. 3rd ACM Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., Seattle, WA, USA, Aug. 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 Conf. Comput. Commun., Mar. 2004, vol. 3, pp. 1705–1716.

[12] Y. Li, Y. Yang, and X. Lu, “Rules of designing routing metrics for greedy, face, and combined greedy-face routing,” IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582–595, Apr. 2010.

[13] R. Shah and J. Rabaey, “Energy aware routing for low energy ad hoc sensor networks,” in Proc. IEEE Wireless Commun. Netw. Conf.,Mar. 17–21, 2002, vol. 1, pp. 350–355.

[14] J.-H. Chang and L. Tassiulas, “Maximum lifetime routing in wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 609–619, Aug. 2004.

[15] H. Zhang and H. Shen, “Balancing energy consumption to maximize network lifetime in data-gathering sensor networks,” IEEE Trans. Parallel Distrib. Syst., 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,” IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 2258–2267, Jul.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 Proc. 19th Int. Conf. Comput. Commun. Netw., Aug. 2010, pp. 1–6.

[18] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy inenergy-constrained sensor network routing,” in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 88–93.

[19] Y. Li and J. Ren, “Preserving source-location privacy in wireless sensor networks,” in Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw., Rome, Italy, Jun. 2009, pp. 493–501.

[20] Y. Li and J. Ren, “Source-location privacy through dynamic routing in wireless sensor networks,” in Proc. IEEE INFOCOM 2010, San Diego, CA, USA., Mar. 15–19, 2010. pp. 1–9.

[21] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks,” in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008, pp. 51–55.

[22] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source-location privacy in sensor network routing,” in Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2005, pp. 599–608.

[23] Wikipedia. Quartic function [Online]. Available: <http://en>. wikipedia.org/wiki/Quartic\_function, Apr. 2014.

[24] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks:Attack and defense strategies,” IEEE Netw., vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[25] A. Pathan, H.-W. Lee, and C. seon Hong, “Security in wireless sensor networks: Issues and challenges,” in Proc. 8th Int. Conf.Adv. Commun. Technol., 2006, pp. 1043–1048.