LIFETIME OPTIMIZATION AND SECURITY IN WSN USING E-CASER PROTOCOL

Veena V.K, S.Subbulakshmi
Department of Electronics and Communication Engineering
Valliammai Engineering College, Kattankulathur, Chennai, Tamilnadu, India
veenapournami@gmail.com, subbujayanth@gmail.com

Abstract— It is well known that wireless sensor networks (WSNs) is a self-organization wireless network system constituted by numbers of energy-limited micro sensors under the banner of industrial application (IA). In this project, we propose a secure and efficient Cost Aware Secure Routing (CASER) protocol to address two conflicting issues; they are lifetime optimization and security. Through the energy balance control and random walking, we can address those conflicting issues. 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.

Index Terms— Routing, security, delivery ratio, energy efficiency.

I. INTRODUCTION

A wireless Sensor Network (WSN) consists of hundreds or thousands of sensor nodes and a small number of data collection devices. The sensor nodes have the form of low-cost, low-power, small-size devices, and are designed to carry out a range of sensing applications, including environmental monitoring, military surveillance, fire detection, animal tracking, and so on. The sensor nodes gather the information of interest locally and then forward the sensed information over a wireless medium to a remote data collection device (sink), where it is fused and analyzed in order to determine the global status of the sensed area. The basic structure of Wireless Sensor Networks is shown in figure 1.1.

In many WSN applications, the sensor nodes are required to know their locations with a high degree of precision, such as tracking of goods, forest fire detection, and etc. For example, in forest fire tracking, the moving perimeter of the fire can only be traced if the locations of the sensors are accurately known. Accordingly, many sensor localization methods have been proposed for WSNs. Broadly speaking, these methods can be categorized as either range-based or range-free. In range-based schemes, the sensor locations are calculated from the node-to-node distances or inter-node angles. Conversely, in range-free schemes, the sensor locations are determined by radio connectivity constraint. Range based schemes are typically more accurate than range-free schemes. However, they require the use of infrared, X-ray or ultrasound techniques to calculate the inter-node distance and/or angle, and are therefore both more complex and more expensive than range-free schemes.

Figure 1.1 Basic structure of a WSN

A key feature of such networks is that each network consists of a large number of un tethered 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 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 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 Resource Conscious Secure routing (RCS) protocol for WSNs without relying on flooding. RCS 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.

II. LITERATURE SURVEY

In Geographic and energy aware routing (GEAR), the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighbouring nodes based on estimated cost and learning cost. Source-location privacy is provided through broadcasting that mixes valid messages with 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 [6], 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. 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 are able to get the direction/sector information stored in the header of the message.

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 [9]. The source chooses the immediate neighbouring node to forward the message based on either the direction or the distance [7], [10], [20], [21]. The distance between the neighbouring nodes can be estimated or acquired by signal strengths or using GPS equipments [3], [17]. The relative location information of neighbour nodes can be exchanged between neighbouring nodes. In [20], 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 for-wards the messages based on greedy geographic routing strategy. A query based geographic and energy aware routing (GEAR) was proposed in [21]. In GEAR, the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighbouring 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 neighbour information, and provide 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 [2], including GEDIR, MFR and compass routing algorithm. The delivery ratio can be improved if each node is aware of its two-hop neighbours. There are a few papers [7], [1], [15], [11] 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 message along one or possibly a sequence of adjacent faces toward the destination.

Lifetime is another area that has been extensively studied in WSNs. In [18], 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 diff-fusion. Then, the routing scheme will choose a path based on a probabilistic method according to the remaining energy. In [4], Chang and Tassiulas 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 neighbouring node selection to maximize the network life-time. Then Zhang and Shen [22] 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. Liu et al. in [12] 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, [5] 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 trace back to the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design [16], [13], [14]. In [19], 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, 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 neighbour 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 are 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 $2^n$.

In [13], [14], 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 [8], 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.

### III. PROPOSED SYSTEM

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 neighbouring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design traffic 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.

#### 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

#### A. Network partition

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 or 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 neighbouring grids. The information maintained by each sensor node will be updated periodically. We assume that the sensor nodes in its direct neighbouring grids are all within its direct communication range. We also assume that the whole network is fully connected through multi-hop communications. In addition, through the maintained energy levels of its adjacent neighbouring grids, it can be used to...
detect and filter out the compromised nodes for active routing selection.

B. Shortest Path Routing

The shortest path routing also called deterministic routing, in this routing the next hop grid is selected from the neighbour grid list based on the relative locations of the grid. The grid that is closest to the sink node is selected for message forwarding and also we are considered energy level of the selected node. The selected nodes have the highest energy level when compared with other node’s energy levels. In this routing we are using cryptographic technique for message security. The deterministic shortest path routing guarantees that the messages are sent from the source node to the sink node.

C. Secure Message Forwarding

This routing is also called random walking, in this routing the next hop grid randomly selected from neighbour grid list for message forwarding. 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. Using this routing we can avoid the jamming.

D. Procedure

- Setup the simulation parameters
- Create the nodes.
- Set the communication range for all nodes
- Find the neighbour node for all the nodes
- Select the neighbour node based on the communication range
- Then calculate the distance from one node another
- Make the cluster formation
- First we need to evenly divide the network area and calculate the energy level for all other nodes
- Select the highest energy node as a cluster head then select the cluster members
- Cluster head collects the information from cluster members
- Finally cluster head transmit collected information to the sink.

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 neighbouring grids. The information maintained by each sensor node will be updated periodically. We assume that the sensor nodes in its direct neighbouring 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 balanced energy consumption throughout the sensor network. In addition, the maintained energy levels of its adjacent neighbouring grids can be used to detect and filter out the compromised nodes for active routing selection.

E. CASER steps

Step 1: Find the neighbour grid for all grid

Step 2: Compute the average remaining energy of adjacent neighbour grid,

\[ \varepsilon_\alpha(A) = \frac{1}{|N_\alpha|} \sum_{i \in N_\alpha} \varepsilon_i \]  

(1)

Step 3: Select the head node based on the highest energy level for packet transmission

\[ N_\text{h}^\alpha = \{ i \in N_\alpha | \varepsilon_i \geq \alpha \varepsilon_\alpha(A) \} \]  

(2)

Step 4: Choose the routing type

Step 5: Select the random number \( \gamma \in [0, 1] \)

Step 6: If \( \gamma > \beta \), the node will send the message through the shortest path, which is deterministic routing

Step 7: Otherwise transmit the packet through the randomly selected neighbouring grid, which is random walk routing.

E. 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 neighbouring grids. For node \( A \), denote the set of its immediate adjacent neighbouring grids as \( N_\alpha \) and the remaining energy of grid \( i \) as \( \varepsilon_i; i \in N_\alpha \). With this information, the node \( A \) can compute the average remaining energy of the grids in \( N_\alpha \) as equation (1).

In the multi-hop routing protocol, node \( A \) selects its next hop grid only from the set \( N_\alpha \) 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 $\alpha = [0, 1]$ to enforce the degree of the energy balance control. We define the candidate set for the next hop node as equation (2) based on the EBC $\alpha$. It can be easily seen that a larger $\alpha$ corresponds to a better EBC. It is also clear that increasing of $\alpha$ may also increase the routing length. However, it can effectively control energy consumption from the nodes with energy levels lower than $\alpha \varepsilon(A)$.

It should be pointed out that the EBC parameter $\alpha$ can be configured in the message level, or in the node level based on the application scenario and the preference. When $\alpha$ 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 $N^A$ shrinks as $\alpha$ increases. In other words, as $\alpha$ increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since $\varepsilon(A)$ is defined as the average energy level of the nodes in $N^A$, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from $N^A$.

F. Secure routing strategy

CASER 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 $N^A$ 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 $N^A$ for message forwarding. The distribution of these two algorithms is controlled by a security level $\beta \in [0, 1]$, 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 $\beta$ is an adjustable parameter. A smaller $\beta$ results in a shorter routing path and is more energy efficient in message forwarding. On the other hand, a larger $\beta$ provides more routing diversity and security.

IV. RESULTS AND DISCUSSION

NS2 is one of the most popular open source network simulators. We conduct the following experiments with ns 2.34 simulator. There are 100 sensor nodes randomly deployed in the communication field. The simulation time is 30ms. We have demonstrated various parameters as follows when compared to CASER [23] protocol and E-CASER protocol.

In CASER protocol they are using same grid head for whole transmission. Here we selected a dynamic head selection based on highest energy in each grid. We are comparing CASER protocol with Dynamic grid head selection. We are using the x-graph for evaluate the performance. Using some evaluation metrics: Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source, End-to-End delay - the average time taken for a packet to be transmitted from source to destination. Packet loss – Total number of packets loss from transmitted packets

A. Packet delivery ratio Vs Time

Figure 2 shows packet delivery ratio of CASER protocol and E-CASER protocol. While analyzing we can see that the E-CASER have 2.92% increment in packet delivery ratio.

B. Packet loss rate Vs Simulation period

Figure 3 shows packet loss rate of CASER protocol and E-CASER protocol. While analyzing we can see that the E-CASER protocol have low packet loss rate. There is 34.62% decrement in proposed scheme
C. E2E Delay Vs Simulation

Figure 4 shows the End to End delay Vs Simulation period. The E-CASER has low E2E delay compared to CASER protocol. There is 34.72% decrement in E-CASER protocol compared to the CASER protocol.

D. Routing Overhead Vs Simulation time

Figure 5 shows routing overhead for E-CASER and CASER protocol. The E-CASER has 1.28% decrement while compared to CASER.
V. CONCLUSION

In this paper, we presented a cost aware secure and efficient routing 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. We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. In experimental results, we can increase the lifetime and the number of messages that can be delivered under the non-uniform energy deployment.

VI. FUTURE WORK

Aggravated by the actuality that WSNs routing is often geography based, we propose geography based secure and efficient Resource Conscious Secure routing (RCS) 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. In the Random walking method, there is a chance of choosing low energy node as a relay node. To avoid this, the data is transmitted via energy aware route only, the MES scheme on Elliptic curve algorithm used to provide authentication. For security purposes, the content of each message can also be encoded by using pattern encoding method and decoded at the sink node by knowing the swapping bit position. So, unauthenticated person cannot access the original data. By this way, the protocol provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks.

REFERENCES


