Security for source node privacy and maximizing network lifetime through routing in Wireless Sensor Networks

Ms. Madhuri Dwarakanath[1]
II SEM, M.Tech, Computer Science and Engineering
City Engineering College
Bengaluru, India

Mrs. Sowmya Naik[2]
Asst. Professor. Dept. of CSE.
City Engineering College
Bengaluru, India

***Abstract*— Sensor networks have been extensively used in various applications because of their ease of installation, cost efficient and portability. Due to the open nature of sensor networks, it is relatively easy to trace packet movement in the network in order to capture the source and destination. Many security protocols have been developed to provide confidentiality for the content of messages, whereas contextual information usually remains exposed. While confidentiality of the message can be ensured through content encryption, it is a challenging task to adequately address the source location privacy. This paper provides a formal model for the source location privacy problem in sensor networks and examines the privacy characteristics of different sensor routing protocols. A novel tree based routing scheme is proposed for preserving source location privacy using hide and seek strategy. The proposed scheme is also efficient in maximizing the lifetime of the network. The main idea is that the lifetime of WSNs depends on the nodes with higher energy consumption. This scheme not only achieves privacy preservation but also network lifetime maximization. Furthermore, a systematic analysis is performed on the energy consumption in WSNs. Theoretical and experimental results show that this scheme is very effective to improve the privacy protection while maximizing the network lifetime.**

Keywords*— Wireless sensor networks, source location privacy, network lifetime, tree based routing.

I. INTRODUCTION

Wireless sensor networks (WSN) is a growing technology which is offering solution for many application areas such as health care, military, industry and also environmental conditions like temperature, sound, gas, pressure. SNs are used for sensing the environments and used to read the sensing information and transmit to base station and also used for monitoring purposes Sensor node is a tiny device includes five basic components 1)controller 2)communication devices 3)sensors/actuators 4) memory 5) power supply. These sensor networks are used for many critical applications where security is also critical and energy replacement is difficult if not impossible. So it is important satisfy application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to extend the system useful period of time. The trade of between energy consumption and gain in reliability gain with goal maximize the WSN system lifetime

On the other hand, security in WSNs is an important issue, especially if they have mission-critical tasks. For instance, a confidential patient health record should not be released to third parties in a heath care application. Securing WSNs is critically important in tactical (military) applications where a security gap in the network would cause causalities of the friendly forces in a battlefield. Security attacks against WSNs are categorized into two main branches: Active and Passive. In passive attacks, attackers are typically camouflaged (hidden) and either tap the communication link to collect data; or destroy the functioning elements of the network. Passive attacks can be grouped into eavesdropping, node malfunctioning, node tampering/ destruction and traffic analysis types. In active attacks, an adversary actually affects the operations in the attacked network. This effect may be the objective of the attack and can be detected. For example, the networking services may be degraded or terminated as a result of these attacks. Active attacks can be grouped into Denial-of-Service, black hole, wormhole, sinkhole, etc.), flooding and Sybil types.

Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively (e.g., information gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks). In a security system, if the first line of defense, "Intrusion Prevention," does not prevent intrusions, then the second line of defense, "Intrusion Detection," comes into play. It is the detection of any suspicious behavior in a network performed by the network members. In any security plan, Intrusion Detection Systems (IDSs) provide some or all of the following information to the other supportive systems: identification of the intruder, location of the intruder (e.g., single node or regional), time (e.g., date) of the intrusion, intrusion activity (e.g., active or passive), intrusion type (e.g., attacks such as worm hole, black hole, sink hole, selective forwarding, etc.), layer where the intrusion occurs (e.g., physical, data link, network). This information would be very helpful in mitigating (i.e., third line of defense) and remedying the result attacks, since very specific information regarding the intruder is obtained. Therefore, intrusion detection systems are very important for network security.

Intrusions over the web have become additional dynamic and complicated. Intrusion detection Systems determines intrusions by scrutiny noticeable behavior against suspicious patterns. There are two types of intrusion detection systems.
Network based IDS**:** these types of IDS are strategically positioned in a network to detect any attack on the hosts of that network. To capture all the data passing through the network, you need to position your IDS at the entry and exit point of data from your network to the outside world. You can also position some IDS near the strategic positions of your internal network, depending on the level of security needed in your network. Since a network based IDS need to monitor all the data passing through the network, it needs to be very fast to analyze the traffic and should drop as little traffic as possible.
Host based IDS: they are installed in a host and they can monitor traffics that are originating and coming to those particular hosts only. If there are attacks in any other part of the network, they will not be detected by the host based IDS.. Apart from monitoring incoming and outgoing traffic, a host based IDS can also analysis the file system of a host, users' logon activities, running processes, data integrity etc.

To address source-location privacy for sensor networks, this paper provides a formal model for the source-location privacy problem and examines the privacy characteristics. We introduce two metrics for quantifying source-location privacy in sensor networks, the safety period and capture likelihood. In our examination of popular routing techniques used in today's sensor networks, we also considered important systems issues, like energy consumption, and found that most protocols cannot provide efficient source-location privacy. New techniques are used to enhance source-location privacy that augment these routing protocols. It is important that this privacy enhancement does not come at a cost of a significant increase in resource consumption. A strategy is devised, called phantom routing, that has proven flexible and capable of preventing the adversary from tracking the source location with minimal increase in energy overhead.

In this paper, a novel tree-based diversionary routing scheme is proposed for preserving source location privacy and maximizing network lifetime in Wireless Sensor Networks (referred to as the tree route, **TR**). TR is different from current studies in which TR creates more diversionary routes than the traditional phantom routing schemes, which greatly improves source location privacy, and at the same time, the network lifetime does not deteriorate with the increase of the number of diversionary routes compared with the traditional routing protocol for privacy preservation.

II. SYSTEM MODEL AND PROBLEM STATEMENT

In order to facilitate the discussion and analysis of source location privacy in sensor networks, we need to select an exemplary scenario that captures most of the relevant features of both sensor networks and potential adversaries in asset monitoring applications. Throughout this paper, we use a generic asset monitoring application, which we have called the Panda-Hunter Game, as well as refer to a formal model for asset monitoring applications that can benefit from source location privacy protection. In this section we introduce the Panda-Hunter Game and the adversary model.

A. The Panda – Hunter Game

In the Panda-Hunter Game, a large array of panda-detection sensor nodes has been deployed by the Save-The-Panda Organization to monitor a vast habitat for pandas. As soon as a panda is observed, the corresponding *source* node will make observations, and report data periodically to the *sink* via multi-hop routing techniques. The game also features a hunter in the role of the adversary, who tries to capture the panda by back-tracing the routing path until it reaches the source. As a result, a privacy-cautious routing technique should prevent the hunter from locating the source, while delivering the data to the sink.

In the Panda-Hunter Game, we assume there is only a single panda, thus *a single source*, and this source can be either stationary or mobile. During the lifetime of the network, the sensor nodes will continually send data, and the hunter may use this to his advantage to track and hunt the panda. We assume that the source includes its ID in the encrypted messages, but only the sink can tell a node's location from its ID. As a result, even if the hunter is able to break the encryption in a reasonably short time frame, it cannot tell the source's location. In addition, the hunter has the following characteristics:

- **Non-malicious:** The adversary does not interfere with the proper functioning of the network; otherwise intrusion detection measures might flag the hunter's presence. For example, the hunter does not modify packets in transit, alter the routing path, or destroy sensor devices.
- **Device-rich:** The hunter is equipped with devices, such as antenna and spectrum analyzers, so that it can measure the angle of arrival of a message and the received signal strength. From these two measurements, after it hears a message, it is able to identify the immediate sender and move to that node. We emphasize, though, that the hunter cannot learn the origin of a message packet by merely observing a relayed version of a packet. In addition, the hunter can detect the panda when it is near.
- **Resource-rich:** The hunter can move at any rate and has an unlimited amount of power. In addition, it also has a large amount of memory to keep track of information such as messages that have been heard and nodes that have been visited.
- **Informed:** To appropriately study privacy, we must apply Kirchhoff's Principle from security to the privacy setting. In particular, Kirchhoff's Principle states that,

in assessing the privacy of a system, one should always assume that the enemy knows the methods being used by the system. Therefore, we assume that the hunter knows the location of the sink node and knows various methods being used by the sensor network to protect the panda.

B. Adversaries Model

Because of the high profits related to Panda hunting, the adversaries would try their best to equip themselves with advanced equipments, which means they would have some technical advantages over the sensor nodes. The adversaries are assumed to have the following capabilities:

1) The adversaries are capable of having sufficient energy resource, adequate computation capability and enough memory for data storage. The adversaries observe the wireless communication within a certain detection range. 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 any delay. We assume that the adversaries will never miss any event when they are close to the event.

2) The adversaries are able to adopt the direction-oriented attack strategy: the adversaries estimate the direction of the source node, and traces along the estimated direction rather than reversely traces hop by hop; and

3) The adversaries will not interfere with the proper functioning of the network, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily detected and could put the adversaries at risk of being caught. However, the adversaries may carry out passive attacks, such as eaves-dropping the communications.

C. Problem Statement

In this paper, we focus on designing routing protocols to protect source location privacy, while maximize the lifetime of WSNs. Thus, our objective function consists of two parts: preserving source location privacy and maximizing network lifetime. The preserving source location privacy of a WSN can be characterized by the performance indicators as explained below:

1) Trace time(denoted as T): trace time is defined as the safety period begins from the moment the adversary initiates the tracing procedure (i.e., eavesdrops on the first packet) and ends at the moment when the adversary captures the source.

Because the frequency source node generates a data packet frequency, so the attacker can only be in one data cycle reverse trace jump, so trace time can also mean path length by reverse tracking. The objective of preserving source location privacy can be expressed as

$$\text{Max}\ (T) = \text{D max}\ (tracetime)$$

2) Lifetime (denoted as l): we denote the network lifetime l as the period from the starting of network operation until the first power outage occurs in WSNs.

III. PROPOSED TREE BASED DIVERSIONARY SCHEME

The proposed scheme satisfies the following principles: (1) The routing trees established are homogeneous, and adversary cannot infer the source location based on the shape of the tree and the historical trajectory of the routing path; (2) The energy consumption of the node in hotspots is not increased and the network lifetime is not decreased; and (3) The abundant energy in the region away from the sink is utilized to build redundancy diversionary routes, so that it is difficult for the adversary to trace to phantom node.

The implementation of TR is divided into two phases to meet the design principles: (1) Establish the backbone route path direct to the network edge based on the existing phantom routes, and improve the historical trajectory in order to avoid direction-oriented attacks so as to establish homogeneous trees; and (2) Establish redundancy diversionary routes as many as possible in regions with abundant energy.

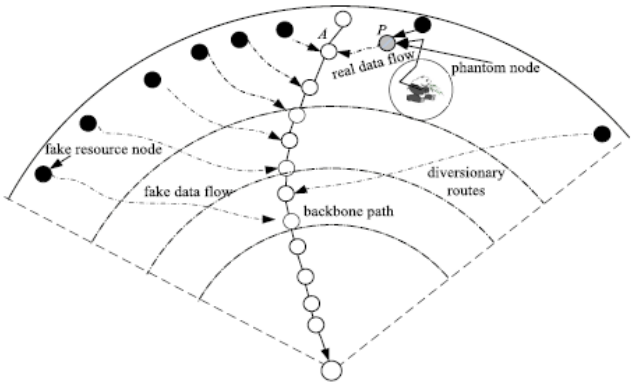

FIGURE 1. Illustrate of the tree-based diversionary routing.

A. OVERVIEW OF THE PROPOSED SCHEME

Tree-based diversionary routing aims at preserving source node privacy and maximizing network lifetime. The main idea is that we establish the phantom node away from the source node and then establish tree routing path towards the sink with strategically created diversionary routes as its branches, also known as diversionary routes. The ends of these diversionary routes are fake source nodes, namely decoy. Our goal is to improve its performance in terms of the following two aspects.

1) PRIVACY

In phantom routes, data of phantom node is sent to the sink according to the shortest routing protocol, therefore the adversaries can trace back to the phantom node. Previous studies have shown that, adversaries can still trace to the source node with a relatively high possibility. Therefore, one possible solution is to make it difficult for adversaries to trace to the phantom node, so that will be impossible to trace the source node. The proposed scheme first establishes a backbone route direct to the network border with diversionary routes as its branches. Then, it establishes diversionary routes as many as possible with each diversionary route directing to the network border, forming a tree based routing path. The data packet length and the data generating possibility are the same in each diversionary route. By doing so, we can achieve relatively high privacy. (A) Firstly, since all routes generated

by the source node are the same tree routing paths, so adversaries cannot speculate the source location based on the routing path. In most current phantom routes, routes generated by different source nodes are not homogeneous. For source node near the sink, its routing path is relatively short, while for that away from the sink, its routing path is relatively long.

Therefore, adversaries can still speculate the approximate location of source node from the length of routing path.

(B) Secondly, since there are many branches in tree routing paths, when adversaries reverse trace, they confront two branches each time, and the probability of right choice is only 1/2. Therefore, for tree routing path with *n* branches, the possibility of adversaries trace to the phantom is very low. The privacy is greatly improved compared with the traditional protocol.

2) NETWORK LIFETIME

The privacy and energy consumption are contradictory. More diversionary routes require extra energy consumption, thus affecting the network lifetime. Generally, after the first nodal death, the network cannot completely and effectively monitor the monitoring area. Therefore, the network lifetime is usually defined as the first node death time. Obviously, to maximize the network lifetime, the key is to reduce the energy consumption in hotspot. Therefore, we minimize the energy consumption in the hotspots and at the same time. Establish diversionary routes by fully using of abundant energy in non-hotspot regions in order to improve the network lifetime.

B. TREE-BASED DIVERSIONARY ROUTING

Based on the network model discussed above, tree based route scheme includes three stages: (1) Tree-based diversionary routing establishment; (2) Stable operation stage of the tree-based routing; and (3) Destruction of tree-based diversionary routing. The requirement of choosing a phantom node is that the phantom node is as far away from the source node. In the following, we will describe the proposed tree-based diversionary routing in details.

1) TREE-BASED ROUTING ESTABLISHMENT

(i) Establish Tree-based diversionary route with phantom Node: First, establish the branch with phantom node, and then establish the tree trunk and other branches. Generally, phantom node cannot be the node on the backbone routing path, because the backbone route is relatively easy to identify, and therefore the phantom node is more vulnerable to be traced. If the phantom node is not on the backbone path, it can be on any existing branches; therefore it is difficult for adversaries to trace. The establishing process of branch with phantom node is as the following two directions (see Fig. 2).

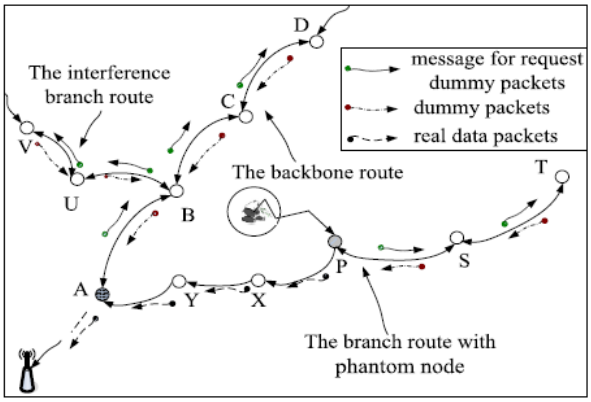

FIGURE 2. The establishing process of tree route.

(A) The left-down direction according to the left-hand rule (Or the right-hand rule): The phantom node *P* selects node *X* from its neighbor nodes, which is the node closest to the sink and on the left (right) of P according to the left-hand rule (or the right-hand rule). Then, *X* selects node *Z* which is on the most right of *X* and with the same hops as *X* to the sink according to the left-hand rule, then selects the most left node closest to the sink, i. e., alternately selects the node closest to the sink and the node with same hops, until the transmission distance reaches the specified hops 8, namely, node *A* in Fig.2, we call it the intermediate node.

```
Algorithm: Adversary Strategy I: Patient Adversary H

next_location = sink;
while (next_location != source) do
    Listen(next_location);
    msg = ReceiveMessage();
    if (IsNewMessage(msg)) then
        next_location = CalculateImmediateSender(msg);
        MoveTo(next_location);
    end
end
```

Algorithm 1: *The adversary waits at a location until it receives a new message.*

(B) The upper right direction of phantom node *P*. *P* sends request packet containing information of request sending dummy packets" to the most right node *S* according to the right hand rule, and the sending frequency of dummy packets is included in the request packet, which indicates node *S* should send dummy data packets to *P* in a fixed time. Similarly node *S* sends request packet to node *T* for dummy data packets, then *T* sends dummy packets to *S*, and so on, until reaching the network border, then the branch route with phantom node is established.

(ii) Establish backbone route with intermediate node.

Assume it starts from intermediate node *A*, then there are also two directions:

(A) The direction from intermediate node *A* to the sink.

Similar with the traditional shortest route protocol, node *A* chooses the neighbor closest to the sink each time, until the packet is sent to the sink.

(B) The opposite direction from node *A* to the sink: Node

A selects the neighbor farthest from the sink as the next hop and sends the request packet node *A* to select the furthest neighbor to the sink as the next hop, and sends request packet containing information of ``request sending dummy packets," node *B* sends dummy packets to *A* in a fixed time after *B* receives the request packet, and the *B* determine whether it has neighbor to the sink farther than itself, if so, node *B* sends the request packet to the furthest neighbor to the sink and so on, until to the network border.

(iii) Establish the diversionary routes. If node *B* on the backbone route is required to establish the diversionary route, node *B* will send request packet containing information of ``request sending dummy packets" to node *U* which has the closest number of hops to the sink with *B*, then node *U* sends dummy packets to *B*. Similarly, node *U* sends request packet to node *V*, and so on, until to the network border, then a branch of diversionary route on 450at the backbone route is established.

2) STABLE OPERATION STAGE OF TREE-BASED ROUTING

In the stable operation stage of the tree route, once all nodes are included in the routes, they operate as the following principle: (a) If the real data packet is received, then the node sends the real data packet when it comes to the transmission time, if not, dummy message is generated in a fixed time and sent when it comes to the transmission time.

3) DESTRUCTION OF TREE-BASED ROUTING

The destruction of tree route is relatively simple, which depends on the phantom node *P*, and intermediate node *A*. If node *P* and node *A* have not received the real data packets within the timeout interval, this routing path will be discarded. Node *P* and node *A* will send message to nodes involved in the route to stop, and once they receive the stop information, they will no longer send any message. Thus, the entire route stops sending message.

```
Algorithm: Adversary Strategy II: Cautious Adversary H(

prev_location = sink;
next_location = sink;
while (next_location != source) do
    reason = TimedListen(next_location, interval);
    if (reason == MSG_ARRIVAL) then
        msg = ReceiveMessage();
        if (IsNewMessage(msg)) then
            next_location = CalculateImmediateSender(msg);
            MoveTo(next_location);
        end
    else
        next_location = prev_location;
        prev_location = LookUpPrevLocation(prev_location);
        MoveTo(next_location);
    end
end
```

Algorithm 2: *The adversary waits at a location for a period of time and returns to its previous location if no message arrives within that period of time.*

IV. CONCLUSION

Source location privacy preservation is becoming more and more important in pervasive computing, and its research is of great significance.

(1) First: The TR scheme has the following advantages over the traditional phantom routing protocol: (A) The route structure is homogeneous, so the adversary cannot speculate the phantom node and source of data, while in previous research, there is only one path in phantom route, and many improved algorithms based on phantom node aim at creating phantom node far away from the source node, so their preservation of the phantom node is weak. (B) This paper analyzes possible adversary models and we identify a new attack called direction-oriented attack, which is a great threat to traditional phantom route protocol, and to the best of our knowledge, previous research all ignored this threat, meanwhile, our scheme can avoid this threat by creating the tree backbone route with left hand rule at probability. (C) The proposed scheme fully uses remaining energy in remote regions to create diversionary routes as many as possible, and with only one route in regions near the sink. This strategy improves the security without affecting network lifetime.

(2) Second, extensive performance analysis of the proposed tree based route scheme shows that tree based route scheme is better than existing privacy preservation protocols. (A) Tree based route scheme has a strong resistance to reverse trace of the adversary , the theoretical and experimental results show that the route length in this paper is more than 10 times of traditional phantom route, which indicts that the adversary has to spend more than 10 times of time to achieve the same effect with phantom route. (B) Tree based route has strong resistance to direction-oriented attack. (C) The proposed scheme has high network lifetime, although the total energy consumption of this scheme is more than 10 times of other protocols, since it maximally reduce the energy consumption in hotspot, the theoretical and experimental results show that the lifetime is the same with phantom route with one route.