Source Location Privacy Preserving of Sensor Nodes using a Tree based Routing Technique for Network Lifetime

Mr. Rakesh Biradar[1] Mr. Atif Afzal Jagirdar[2]
[1,2]Secab Institute of Engineering and Technology, Bijapur

Abstract— In sensor networks, location plays a vital role during communication between the sensor nodes. Preserving security on location of Sensor nodes plays important role for preventing the node duplication attack. Sharing the location of sensor nodes with each other requires the nodes to be active and alive that is they have enough energy to communicate. Over the past few years researchers have been involved in conserving energy by designing and proposing techniques that consume less energy for location sharing. However, one critical challenge to WSNs implementation is source location privacy. In this project, we propose a novel tree-based diversionary routing scheme for preserving. The proposed scheme is able to maximize the network lifetime of WSNs. We propose quadrant based approach to preserver source location privacy using hide and seek strategy to create diversionary or decoy routes along the path to the sink from the real source, where the end of each diversionary route is a decoy (fake source node), which periodically emits fake events. Meanwhile, The main idea is that the lifetime of WSNs depends on the nodes with high energy consumption or hotspot, and then the proposed scheme minimizes energy consumption in hotspot and creates redundancy diversionary routes in nonhotspot regions with abundant energy. Hence, it achieves not only privacy preservation, but also network lifetime maximization. Furthermore, this can also provide security to data transfer using Elliptical curve Cryptography technique.

Key words: Wireless Sensor networks (WSNs), Tree-Based Diversionary Routing

I. INTRODUCTION

Wireless Sensor networks (WSNs) rely on wireless communication, which is a kind of broadcasting media and vulnerable to be eavesdropped. The adversaries may use expensive radio transceivers to interact with the networks and to detect the message flow, and then trace back to the message source by moving along the reversed path even if strong data encryption is utilized. The object, e.g., the endangered animal species, or a vehicle of military aides, may have to be protected for safety reasons and the related location information should not be disclosed. This concern will become even more serious for future sensor network prevalence in pervasive computing applications, as the ubiq uitous information collections doubtlessly encroaches on the privacy of the people involved.Many techniques to address the source location privacy issue have been proposed, where phantom routing is one of the popular approaches for preserving privac . The source location privacy preservation is to hide the physical location of the message source and makes it more difficult for an adversary to trace messages back to the source location. In phantom routing, instead of source node's directly sending its data to the sink, the source first forwards the data to a phantom node which is located away from it, and then the phantom node acts as a decoy relaying the data in a shortest path to the sink. Due to the fact that the currently existing phantom routing scheme always has the phantom node routed to the sink directly, it allows the adversary trace back along the route to phantom nodes, which could result in that the target can be found at last. Obviously, an enhancement routing scheme is to make it difficult for the adversary to trace back to the phantom node, and as a result, the source location cannot be traced and then is protected. A straight-forward solution is to have several diversionary routes to the sink. It is difficult for the adversary to determine which route is the actual data in. So the source location privacy is improved. Unfortunately, another critical issue arises due to the fact that the energy consumption of establishing n diversionary routes can be n times of a single phantom routing. Despite an improvement in source location privacy, the network lifetime could be only 1=n of the single phantom routing.

II. PROBLEM STATEMENT

In this project, 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:

A. Trace Time (Denoted As T):

The 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

$$\max(T) = \max(tracetime)$$

B. Lifetime (Denoted As`):

Since the outage of sensor nodes may have significant impacts on network coverage and communications, we denote the network lifetime as the period from the starting of network operation until the first power outage occurs in WSNs. Let Ei denote the energy consumption of node i]. The objective of maximizing

network lifetime can be expressed as

$$\max(\ell) = \min \max_{0<i\leq n} (E_i)$$

Obviously, the main goal of TR scheme can be stated as follows:

$$\begin{cases} \max(\ell) = \min \max\limits_{0<i\leq n} (E_i) \\ \max(T) = \max(tracetime) \end{cases} \quad (3)$$

III. LITERATURE SURVEY

A. K. Bicakci, H. Gultekin, B. Tavli, And I. E. Bagci, ``Maximizing Lifetime Of Event-Unobservable Wireless Sensor Networks''

Introduced a filtering scheme called OFS (Optimal Filtering Scheme) to maximize the network lifetime and preserve event-unobservability against global eaves droppers.

B. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, And G. Cao, ``Towards Event Source Unobservability With Minimum Network Traffic''

As an enhancement, a proxy-based filtering protocol is proposed. where some sensor node as proxy can filter out fake data packets, thereby reducing network traffic to some extent.

C. M. Shao, Y. Yang, S. Zhu, And G. Cao, ``Towards Statistically Strong Source Anonymity For Sensor Networks''

Proposed FitProbRate protocol. By adjusting the nodal data trans-mission rate, the source location privacy can be preservedand the transport delay can be also reduced.

D. P. Kamat,Y. Zhang,W. Trappe, And C. Ozturk, ``Enhancing Source-Location Privacy In Sensor Network Routing''

Introduced the Panda-Hunter game model for source location privacy. In this model, a large number of sensor nodes are deployed tomonitor the wild habits of Panda. Once the behavior of Panda is monitored, the node nearest to the Panda will report to the base station. The hunter watch near the sink can locate the source node by tracing in the reverse direction hop-by-hop and try to capture the Panda et al. proposed a more well-known phantom routing protocol to against eavesdropping attacks to the source location. However, the phantom node by the first proposed routing is closer to the source node, and as a result the source location may still be easily found by the attacker.

E. H. Chen And W. Lou. (2014). On Protecting End-To-End Location Privacy Against Local Eavesdropper In Wireless Sensor Networks

Proposed four location privacy protection schemes are called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively. Among them, both DBT scheme and ZBT scheme build some branch routes in the route from the real source node to Sink node to improve the privacy protection performance. In the DBT scheme, real messages are delivered along the shortest path, making it possible for the eavesdropper to infer the location of the source or sink by extending the line of the shortest path. So, a proxy source and a proxy sink are adopted in the ZBT scheme, which prevents the adversary from inferring the location of the source or sink easily.

The fake source idea is proposed to make the sensor network have more sources which generate fake messages that have the same size of the real messages and encrypted as well so that an adversary cannot differentiate between the real message and the fake one.

F. Jhumka, M. Bradbury, And M. Leeke. (2014). Fake Source-Based Source Location Privacy In Wireless Sensor Networks:

Proposes a hybrid source location privacy technique. In their approach, temporary and permanent fake sources are modelled as fake sources with varied duration. So, the problem of selecting temporary and permanent fake sources is then directly addressed.

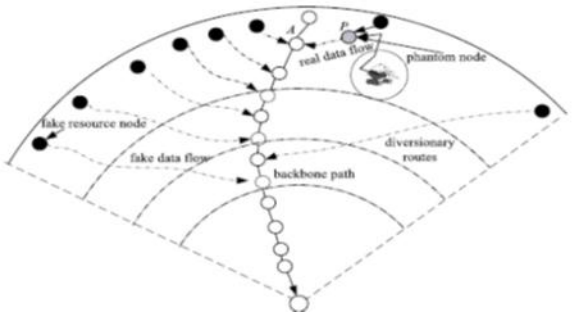
IV. PROPOSED SYSTEM

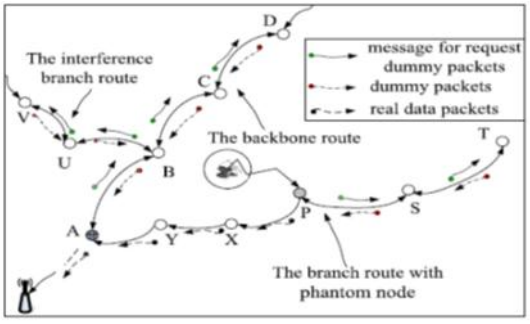
We propose a novel tree-based diversionary routing scheme for preserving source location privacy and maximizing network lifetime in Wireless Sensor Networks (referred to as the tree route, TR). TR is different from current studies in which TR creates more diversionary routes than the traditional phantom 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.

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.
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.
4) The System Provides Secure Data Transfer via Elliptical Curve Cryptography (ECC) which allows encryption and decryption without key exchange.
5) The Quadrant routing approach allows creation of tree based routing approach while preserving location privacy.

A. System Architecture:





B. Working Principle:

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 which will be discussed in detail later, so as to establish homogeneous trees according to principle 1
2) Establish redundancy diversionary routes as many as possible in regions with abundant energy to meet principle 2 and principle 3. decoy. Our goal is to improve its performance in terms of the following two aspects.

V. 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.

A. 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. 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.

1) 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.
2) 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.

B. Network Lifetime:

In many existing studies, 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.

VI. 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.
3) Destruction of tree-based diversionary routing. It is worth noting that we adopt the same method of creating a phantom node from. 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.

A. Implementation Details System Requirements:

1) Hardware Requirements:

- Processor: Pentium 3 or More.
- Ram: 512MB or More.
- Hard Disk: 200MB.

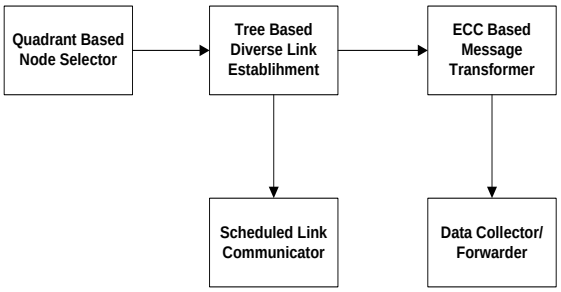
2) Software Requirements:

- JAVA (JDK 1.6 or More).
- NetBeans IDE 6.1 or More.
- Programming language JAVA.
- Atarraya Simulator Tool.

3) Modules:

- Quadrant based Node Selector.
- Tree based Diverse Link Establisher.
- Scheduled Link Communicator.
- ECC Based Message Transformer.
- Data Collection/Forwarder.

4) Module Flow Diagram:



5) Advantages:

1) 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.

2) 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.

VII. CONCLUSION

- We planned to implement a Source Location Privacy Preserving of Sensor Nodes using a Tree based for Prolonged Network Lifetime.
- The main idea is that the lifetime of WSNs depends on the nodes with high energy consumption or hotspot, and then the proposed scheme minimizes energy consumption in hotspot and creates redundancy diversionary routes in nonhotspot regions with abundant energy.
- Furthermore, this can also provide security to data transfer using Elliptical curve Cryptography technique.

REFERENCES

[1] K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, ``Maximizing lifetime of event-unobservable wireless sensor networks"
[2] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, ``Towards event source unobservability with minimum network traffic"
[3] M. Shao, Y. Yang, S. Zhu, and G. Cao, ``Towards statistically strong source anonymity for sensor networks"
[4] P. Kamat,Y. Zhang,W. Trappe, and C. Ozturk, ``Enhancing source-location privacy in sensor network routing"
[5] Jhumka, M. Bradbury, and M. Leeke. (2014). Fake source-based source location privacy in wireless sensor networks.

