A Novel Method to Achieve Source Location Privacy in Wireless Sensor Networks

Shruthi P M.Tech 4th sem SJBIT
Kiran Kumar Asst.Prof, SJBIT, Bangalore

Abstract:- **Wireless sensor networks have found wide applications in many areas. The key challenge in implementation of wireless sensor networks is to hide the location of the source by sending data in multiple paths from the source node to sink. This way attackers will not be able to trace back to the source node. The end of this multiple paths will be fake source nodes which will periodically generate fake messages. This scheme will also maximize the network lifetime. Usually in wireless sensor networks the nodes near the sink will be hotspots and energy is consumed more in that region. So the proposed scheme will reduce the energy consumption in hotspots by building multiple paths in non hotspot regions with abundant energy. This proposed method is effective against direction oriented attacks.**

Index Terms :- Wireless Sensor networks, Source location privacy, trace time

I. INTRODUCTION

Wireless sensor network is a kind of broadcasting media which depends on wireless communication and it is susceptible to eavesdropping. The attackers may use expensive transceivers to detect the flow of data and trace back to the source node. While detecting any endangered species or military objects it must be protected from attackers and location of those species or objects must not be disclosed. Hence it is important to preserve the location of source node. In the existing methods instead of source node routing directly to the sink it will first send to phantom node which then sends the data to the sink using the shortest path. But this method is not that effective as the attacker can eventually trace back to the source node. Obviously an enhancement to this method would be to send the data in multiple paths so that it will be difficult for the attacker to determine in which path the actual data is. Thus source location privacy achieved.

II. SYSTEM MODEL AND PROBLEM STATEMENT

A. SYSTEM MODEL

1) NETWORK MODEL The following assumptions are made about the network

1) The sensor nodes in the network are randomly distributed, and the communication range of each sensor node is equal.
2) The sensor nodes know their locations and the sink node location. Each sensor node has the knowledge of its neighboring nodes**.**
3) A secure communication is already implemented and no contents of the packets are disclosed.

B. ATTACKER MODEL The attackers are capable of the following

1) The attackers have sufficient energy and computation capability.
2) On detecting an event, they attackers can determine the sender by analyzing the direction and strength of the signal received.
3) The attackers will not interfere with the proper functioning of the network, such as modifying packets or the routing path, or disabling the sensor devices, since such activities can be easily detected and could put the attackers at risk of being caught.

B PROBLEM STATEMENT

Objective function consists of two parts: Hiding the location of source and maximizing the network lifetime. This can be characterized by the following performance indicators

1) Trace time: The time taken by the attacker to trace back and reach the source node. The trace time depends upon the path length.
2) Network lifetime: the network lifetime is defined as the period from the starting of network operation until the first nodal death.

III. PROPOSED SCHEME

We propose a novel method to achieve source location privacy. The proposed fulfills the following principles

1) The multiple paths established are homogeneous, and attacker cannot determine the source location based on the shape of the paths and the historical trajectory of the routing paths.
2) The energy consumption of the node in hotspots is decreased and the network lifetime is increased.
3) The abundant energy in the region away from the sink is utilized to build redundant paths, so that it is difficult for the attacker to trace back to the source node.

The novel method is implemented in three phases

1) Create fake source nodes at network border.
2) Build a backbone path.
3) Build redundant paths as many as possible in regions with abundant energy to meet principle 2 and 3.

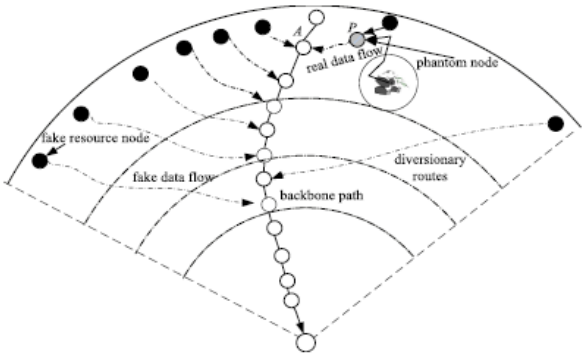

Figure 1: Illustration of multipath routing

A. OVERVIEW OF PROPOSED SCHEME

The proposed scheme aims at preserving source node privacy and maximizing network lifetime. The main idea is that we establish multiple paths towards the sink . The ends of these multiple routes are fake source nodes. 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 attackers can trace back to the phantom node. Previous studies have shown that, attackers can still trace to the source node with a relatively high possibility. Therefore, one possible solution is to make it difficult for attackers to trace to the phantom node, so that will be impossible to trace the source node. The proposed scheme first establishes a backbone route to and then establishes multiple routes with each route directing to the network border. The length of the data packet and the frequency of data generation is 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 homogeneous, so attackers 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, attackers can still speculate the approximate location of source node based on the length of routing path.

(B) Secondly, since there are many paths, when attackers reverse trace, they confront two paths each time, and the probability of right choice is only half. Therefore, for routing path with *n* paths, the possibility of attackers trace to the source node is very low. The privacy is greatly improved compared with the traditional protocol.

2) 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 energy in the hotspot has to be reduced. Hence, the energy consumption in the hotspots is reduced and at the same time establish multiple diversionary routes by fully using of abundant energy in non-hotspot regions in order to improve the network lifetime.

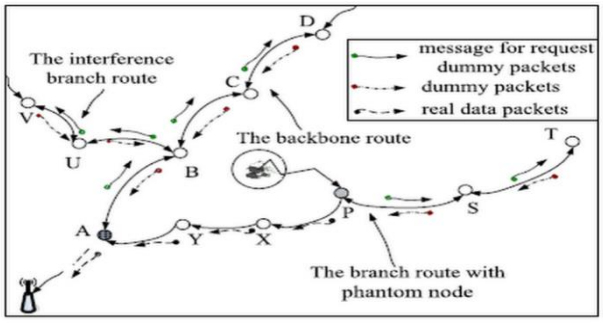

Figure 2: Establishment of route

B. MULTIPATH DIVERSIONARY ROUTING

Based on the network model discussed above, multipath routing scheme includes three stages: (1) Multipath diversionary route establishment; (2) Stable operation stage of the multipath diversionary routes; (3) Destruction of multipath diversionary routes.

VI. EXPERIMENTAL RESULTS

A. ANALYSIS OF TRACE TIME

We determine the optimal routing strategies based on two performance metrics: mean trace time and minimum trace time. The frequency of data generation by the source node is denote by f , then the time interval of the data generation is give by Tc=1/f. This indicates that a data packet will be generated during every Tc.

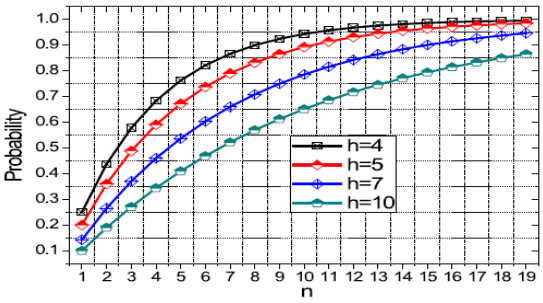

Figure 3: Relationship between trace route and success probability

Fig. 3 shows success probability under different trace paths number *n* and different hops *h* from the sink to the source node. As shown, the success rate is higher when *n* is bigger, and the success rate is lower when *h* is bigger. If *h*=4, the success rate can be 68.359% when *n*=4, and the success rate can be 94.369% when *n* =10. Meanwhile, when the distance from the sink to the source node is more than 4 hops, both theoretical and practical results have demonstrated that if the message is randomly routed for *h* hops, then the message will largely be within *h* hops away from the actual source node. Therefore, to meet the condition where *h is* 4, the message has to be routed

randomly for 16 hops, but even in such a situation, the attacker only needs 4 tracing routes, the success probability can be 68.359%. Obviously, the direction-oriented attack is a bit threat to source location privacy.

B. EXPERIMENTAL RESULTS OF ENERGY CONSUMPTION AND NETWORK LIFETIME

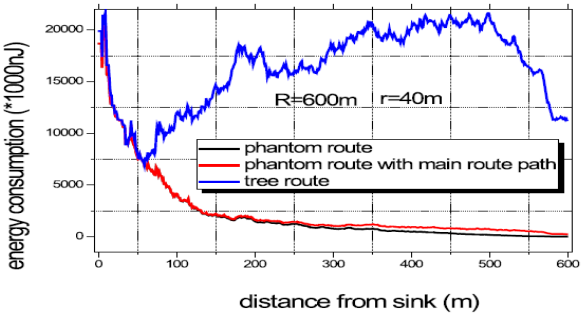

Figure 4: consumption of energy under different protocols

Fig. 4 shows the energy consumption in different regions under phantom route and multipath route. The experimental scene is that we randomly choose two hundred source nodes in the network, and then experiments are conducted on each node. In Fig. 4 the phantom route refers to the route from phantom node created near the source node to the sink. As can be seen from Fig. 4 under phantom route protocol, the energy consumption near the sink is quite big, and small for regions away from the sink near the network border, so its energy efficiency is not high. While under the multipath routing scheme in this paper, the energy consumption is also high for regions in the network border away from the sink, as long as the energy consumption in hotspots is not exceeded, the network lifetime will not be affected. Therefore, we create multiple diversionary routes as many as possible by fully using energy in regions away from the sink, since there is only one path near the sink in the hotspots, the energy consumption in hotspot is the same with that under phantom route protocol, thus the lifetime is the same. The experimental results in Fig. 4 show the route scheme in this paper greatly improves the network security by creating more diversionary routes without affecting the network lifetime. Since in multipath routing scheme energy consumption is balanced in all regions achieving high energy efficiency.

Fig. 5 shows the total energy consumption under tree based route and phantom route. As can be seen from Fig. 13, the energy

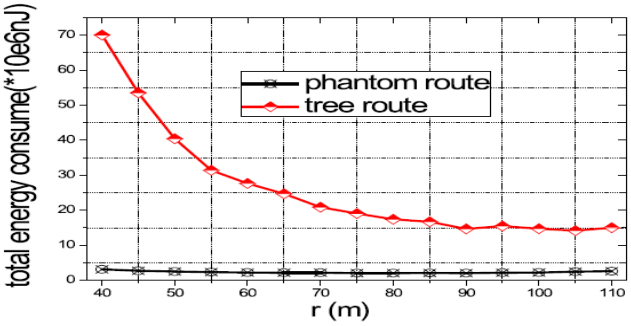

Figure 5: Energy consumption

consumption with multipath routing is 4.7 times to 21.7 times of the energy consumption with phantom route, this is because the tree based route scheme creates many diversionary routes, and then the energy consumption is increased by times, since this increased energy consumption is in the outside region, so this has no effect on the network lifetime.

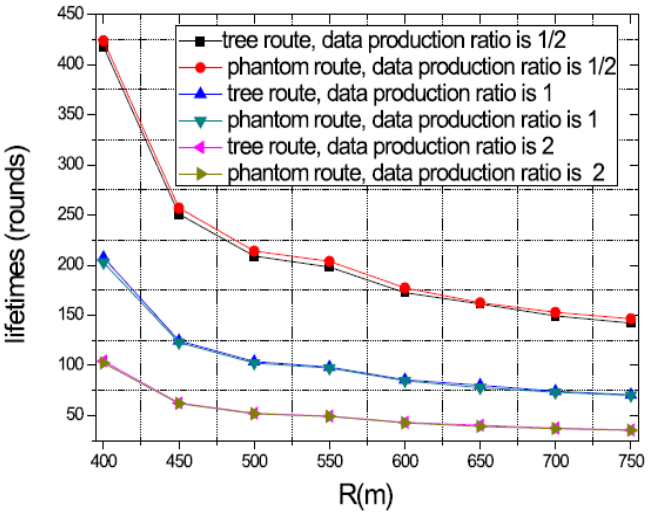

Figure 6: Relationship between network lifetime and source node data transmission frequency

Fig. 6 shows the relationship between network lifetime and number of tree created under certain data transmission frequency.

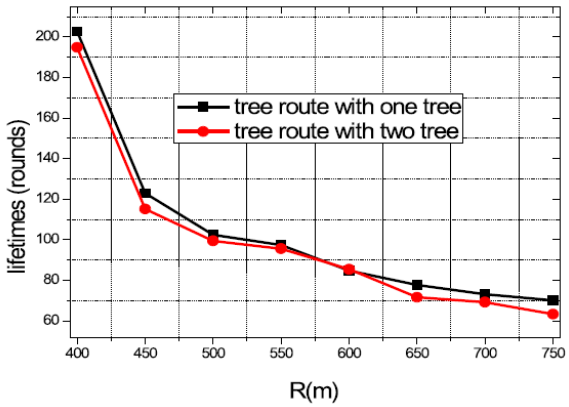

Figure 7: Comparision of network lifetime under multiple trees

As shown Fig. 7, to create more trees on the same source node has little effect on the network lifetime. The main reason is as the following. When *m* trees are created, the data transmission frequency is only 1=*m* of the original, so the energy consumption is only 1=*m* of the original, since there are *m* trees, the total energy consumption remain the same, this shows more routes do not affect network lifetime. And through more trees, the network security is improved.

CONCLUSION

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

(1) First: The multipath routing scheme has the following advantages over the phantom routing protocol: (A) The route structure is homogeneous, so the attacker cannot speculate th 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 analyses possible attacker models and we identify a new attack called direction-oriented attack, which is a great threat to traditional phantom route protocol, and the previous researchers have all ignored this threat, meanwhile, our scheme can avoid this threat by creating multiple routing paths. (C) The proposed scheme fully uses remaining energy in remote regions to create diversionary routes as many as possible, and with a single route in regions near the sink. This strategy improves the security without affecting network lifetime. (2) Second, extensive performance analysis of the proposed route scheme shows that multipath based route scheme is better than existing privacy preservation protocols. (A) Multipath based route scheme has a strong resistance to reverse trace of the attacker , the theoretical and experimental results. (B) Multipath 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 maximumly reduce the energy consumption in hotspot, the theoretical and experimental results show that the lifetime is the same with phantom route with one route.

REFERENCES

[1] Industrial Wireless Sensor Networks: Applications, Protocols, and Standards [Book News] Silva, F. Industrial Electronics Magazine, IEEE Volume:8, Issue: 4 2014.

[2] Maintaining Quality of Sensing with Actors in Wireless Sensor Networks Shibo He ; Jiming Chen ; Peng Cheng ; Yu Gu ; Tian He ; Youxian Sun Parallel and Distributed Systems, IEEE Transactions on Volume:23, Issue: 9 2012.

[3] Overview of Security Issues in Wireless Sensor Networks Modares, H. ; Salleh, R. ; Moravejosharieh, A. Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference.

[4] A comparative analysis of routing techniques for Wireless Sensor Networks Raghunandan, G.H. ; Lakshmi, B.N. Innovations in Emerging Technology (NCOIET), 2011 National Conference.

[5] A preliminary study on lifetime maximization in clustered wireless sensor networks with energy harvesting nodes Pengfei Zhang ; Gaoxi Xiao ; Tan, H. Information, Communications and Signal Processing (ICICS) 2011 8th International Conference'.

[6] Credit routing for source-location privacy protection in wireless sensor networks Zongqing Lu ; Yonggang Wen Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference.

[7]Cluster based Location privacy in Wireless Sensor Networks against a universal adversary George, C.M.; Kumar, M. Information Communication and Embedded Systems (ICICES), 2013 International Conference.

[8] Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks Yun Li ; Jian Ren ; Jie Wu Parallel and Distributed Systems, IEEE Transactions on Volume:23, Issue: 7, 2012.