I J C T A, 9(14) 2016, pp. 6441-6447

Privacy of Source Location tracking and Improving the Life Time of Network in WSN's Technology

Suryakumar[*] and Arulprakasham[**]

ABSTRACT

Wireless sensor networks (WSNs) have been proliferating due to their wide applications in both military and commercial use. However, one critical challenge to WSNs implementation is source location privacy. In this paper, we propose a novel tree-based diversionary routing scheme for preserving 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 proposed scheme is able to maximize the network lifetime of WSNs. 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 non-hotspot regions with abundant energy. Hence, it achieves not only privacy preservation, but also network lifetime maximization. Furthermore, we systematically analyze the energy consumption in WSNs, and provide guidance on the number of diversionary routes, which can be created in different regions away from the sink. In addition, we identify a novel attack against phantom routing, which is widely used for source location privacy preservation, namely, direction-oriented attack. We also perform a comprehensive analysis on how the direction-oriented attack can be defeated by the proposed scheme. Theoretical and experimental results show that our scheme is very effective to improve the privacy protection while maximizing the network lifetime.

***Index Terms*:** Wireless sensor networks, tree based routing, source location privacy, network lifetime, Performance optimization.

1. 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 now, and then trace back to themessage 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 ubiquitous 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 privacy. 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

[*] M. TECH (final year), *E-mail: Surya.kk29@mail.com*

[**] Assistant Professor, SRM University

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-forwardsolution is to have several diversionary routes to the sink. It is difficult for the adversary to determine which route the actual data is 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. In this paper, 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 life time does not deteriorate with the increase of the number of diversionary routes compared with the traditional routing protocol for privacy preservation.

The privacy threats that exist in wireless sensor networks can be broadly classified along two dimensions, namely

(i) Content-based privacy threats and

(ii) Context-based privacy threats.

While content-based threats are well understood, with cryptographic techniques often being used to address these problems, cryptographic techniques do not address context based threats and context-based privacy has greater challenge. One important aspect of context based privacy in several applications is source location privacy.

2. SYSTEM ANALYSIS

2.1. Existing system

- The TR scheme has the following advantages over the traditional phantom routing protocol:

1. The route structure is homogeneous, so the adversary cannot speculatethe 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. This project analyzes possible adversary models and we identify a new attack calledDirection-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.

2.2 Limitations of Existing system

- Existing approaches are not scalable
- They not cover group communication
- It affects networks lifetime

2.3 Proposed System

- 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.
- 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 maximum reduce the energy consumption in hotspot, the theoretical and experimental results show that the lifetime is the same with phantom route with one route.

2.4 Advantages of Proposed System

- Improves the security
- Without affects the network lifetime

3. SYSTEM MODEL AND PROBLEM STATEMENT

3.1. System Model

1) Network Model

We make the following general assumptions about our network model:

1) Our network model is similar to the explanatory PandaHunter Game that was introduced in [5], [6], [23], and [26]. In this Panda-Hunter Game, a sensor network is deployed with nodal density to continuously monitor activities and locations of the animals in a wild animal habitat. As soon as a Panda is discovered [5], [6], the corresponding source node in the nearby area will observe and report data periodically to the sink node [6], [14];
2) The positions of the target in the network are randomly distributed, i.e., the probability of each sensor node to monitor the target is equal, and then the probability of generating data to the sink is equal [27], [28];
3) The sensor nodes know their relative locations and the sink node location. Each sensor node has the knowledge of its adjacent neighboring nodes. The information about the relative location of the sensor domain may also be broadcasted through this network for routing information update [29][31]; and
4) A security infrastructure, secure communication, has already been in place. In other words, no information carried in the message (e.g., packet head) will be disclosed. The key management, including key generation, key distribution and key update, is beyond the scope of this paper. However, the interested readers are referred to references such as [10] and [25].

3.2. Tree-based Diversionary Scheme

A novel tree-based diversionary routing scheme for preserving source location privacy and maximizing network lifetime. The proposed scheme satises 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 difcult 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 which will be discussed in detail later, so as to establish homogeneous trees according to principle 1; and (2) Establish redundancy diversionary routes as many as possible in regions with abundant energy to meet principle 2 and principle 3.

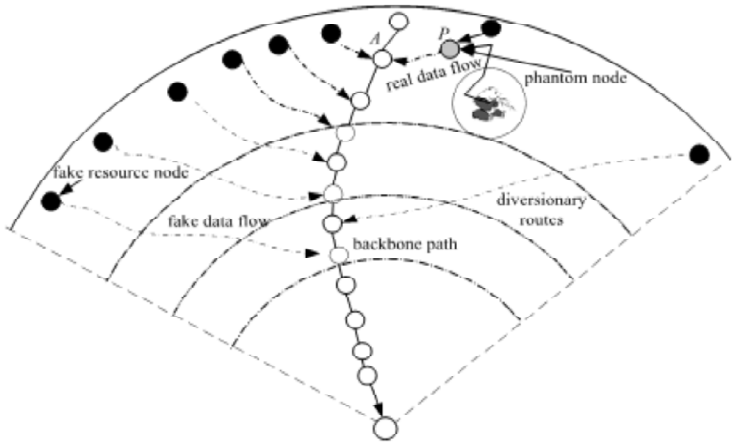


Figure 1: Illustrate of the tree-based diversionary routing

3.3. Technology Used

THE NETWORK SIMULATOR 2.35 (NS2)

3.3.1. The Network Simulator 2.35 (NS2)

Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is part of the VINT project. The goal of NS2 is to support networking research and education. It is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed freely and open source. A large amount of institutes and people in development and research use, maintain and develop NS2. This increases the confidence in it. Versions are available for FreeBSD, Linux, Solaris, Windows and Mac OS X.

3.3.2. Structure of NS2

NS2 is built using object oriented methods in C++ and OTcl (object oriented variant of Tcl.

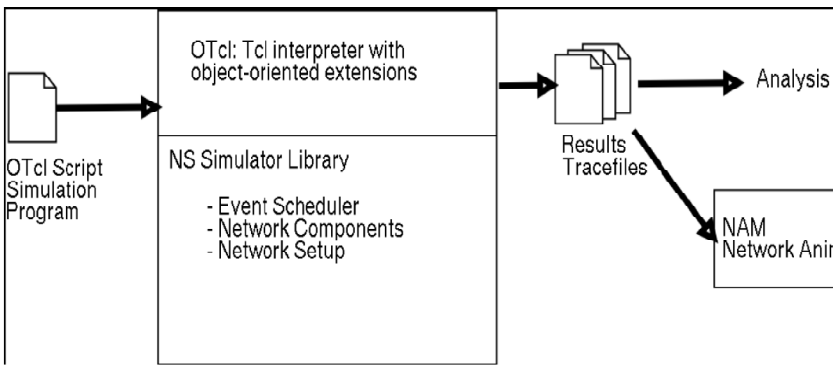


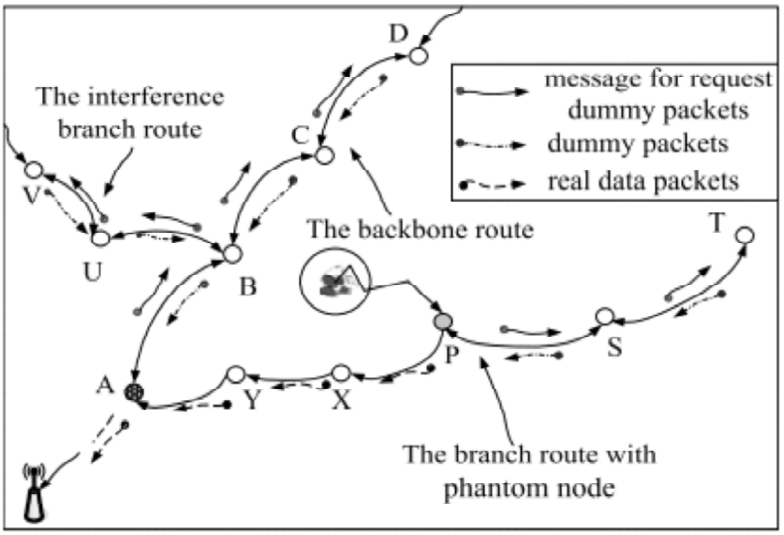
Figure 3.1: Simplified User's View of Ns

can see in Fig 5.1, NS2 interprets the simulation scripts written in OTcl. A user has to set the different components (e.g. event scheduler objects, network components libraries and setup module libraries) up in the simulation environment. The user writes his simulation as a OTcl script, plumbs the network components together to the complete simulation. If he needs new network components, he is free to implement them and to set them up in his simulation as well. The event scheduler as the other major component besides network components triggers the events of the simulation (e.g. sends packets, starts and stops tracing). Some parts of NS2 are written in C++ for efficiency reasons. The data path (written in C++) is separated from the control path (written in OTcl). Data path object are compiled and then made available to the OTcl interpreter through an OTcl linkage (tclcl) which maps methods and member variables of the C++ object to methods and variables of the linked OTcl object. The C++ objects are controlled by OTcl objects. It is possible to add methods and member variables to a C++ linked OTcl object.

4. FUNCTION DIAGRAM

4.1. Tree- route

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 dif-cult for adversaries to trace. The establishing process of branch with phantom node is as the following two directions



4.2. Diagram explanation

(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 neighbour 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 specied hops 8, namely, node A in Fig.2, we call it the intermediate node.

(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 xed 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.

5. SYSTEM DESIGN DETAILS

5.1. Modules

- Hide strategy
- Seek strategy
- Create diversionary routes

5.2. Modules explanation

5.2.1. Hide Strategy

- the proposed scheme is able to maximize the network lifetime of WSNs. 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, we systematically analyze the energy consumption in WSNs, and provide guidance on the number of diversionary routes, which can be created in different regions away from the sink. In addition, we identify a novel attack against phantom routing, which is widely used for source location privacy preservation, namely, direction-oriented attack.

5.2.2. Seek strategy

- We also perform a comprehensive analysis on how the direction-oriented attack can be defeated by the proposed scheme. Theoretical and experimental results show that our scheme is very effective to improve the privacy protection while maximizing the network lifetime**.**

5.2.3. Create diversionary routes

- one critical challenge to WSNs implementation is source location privacy. In this paper, we propose a novel tree-based diversionary routing scheme for preserving 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.

6. CONCLUSION AND FUTURE ENHANCEMENT

Providing location privacy for the source or sink node is very significant in wireless sensor network. An adversary who has knowledge about the network can use location information and easily attack either source node or destination node. In this paper, intervallic gathering, source imitation, sink imitation, backbone flooding are proposed to safe guard the wireless sensor network against global adversaries. There are a number of ways that worth studying in the future. In particular, in this paper, we assume that the global adversary will not negotiate any of the sensor nodes; they only perform traffic analysis without observing the content of the packet. However, in practice, the global adversary may be able to negotiate a few sensor nodes in the field and perform traffic analysis with additional information from insiders.

REFERNCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393422, Apr. 2002.

[2] S. He, J. Chen, Y. Sun, D. K. Y. Yau, and N. K. Yip, "On optimal information capture by energy-constrained mobile sensor," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 24722484, Jun. 2010.

[3] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Netw., vol. 7, no. 8, pp. 15011514, 2009. VOLUME 2, 2014 649

[4] A. Jhumka, M. Leeke, and S. Shrestha, "On the use of fake sources for source location privacy: Trade-offs between energy and privacy,'' Comput. J., vol. 54, no. 6, pp. 860874, 2011.

[5] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of sourcelocation privacy schemes for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 13021311, Jul. 2012.

[6] 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., Columbus, OH, USA, Nov. 2005, pp. 599608.

[7] A.-F. Liu, P.-H. Zhang, and Z.-G. Chen, "Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks," J. Parallel Distrib. Comput., vol. 71, no. 10, pp. 13271355, 2011.

[8] A. Jarry, P. Leone, S. Nikoletseas, and J. Rolim, "Optimal data gathering paths and energy-balance mechanisms in wireless networks," Ad Hoc Netw., vol. 9, no. 6, pp. 10361048, 2011.

[9] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382401, 1982.

[10] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacypreserving scheme against global eavesdropping for ehealth systems," IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 365378, May 2009.

[11] K. Pongaliur and X. Li, "Maintaining source privacy under eavesdropping and node compromise attacks,'' in Proc. IEEE INFOCOM, Shanghai, China, Apr. 2011, pp. 16561664.

[12] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energyconstrained sensor network routing," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw. (SASN), vol. 4. 2004, pp. 8893.

[13] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proc. 6th Annu. IEEE Commun. Soc. Conf. Sens. Mesh Ad Hoc Commun. Netw., Jun. 2009, pp. 19.

[14] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," Comput. Netw., vol. 53, no. 9, pp. 15121529, 2009.