Scientific Journal of Impact Factor (SJIF) : 3.134

ISSN (Print) : 2348-6406
ISSN (Online): 2348-4470

International Journal of Advance Engineering and Research Development

Volume 1, Issue 11, November -2014

A Survey on Achieving Source Location Privacy and Network Lifetime Maximization in Wireless Sensor Networks

Pooja K Akulwar [1], Disha Deotale[2]

[1] Department of Computer Engineering, GHRIET, Pune, poojaakulwar13@gmail.com
2 Department of Computer Engineering, GHRIET, Pune, dishadeotale@raisoni.net

Abstract *— In recent years, Wireless Sensor Network has drawn considerable attention from research community due to wide range of applications used. The most notable challenge which is threatening the WSN is source location privacy. Preserving the source location means hiding the physical location of the source from the adversaries and increasing difficulty for adversaries in tracing the message path back to the source location. Although many of the privacy related schemes such as Phantom routing has been established, still there exists problem with source location privacy. This paper focuses on one solution namely Tree-based Diversionary Routing scheme. The main goal of Tree based diversionary routing is to improve performance in two aspects: privacy and network lifetime. The idea behind Tree-based Diversionary Routing scheme is to create diversionary routes along the path from source to sink and at the end of each route, Fake node is present. This increases difficulty for adversaries in tracing the path and identifying the source node. At the same time, Network Lifetime is also maximized by minimizing the energy consumption in hotspot region and utilizing that energy in creating the diversionary routes in non-hotspot region. The Directed oriented attack which leads the adversaries to identify source node easily can also be avoided*.

Keywords*- Wireless Sensor Network, Phantom routing, Tree-based Diversionary Routing, Network Lifetime, Directed oriented attack*

I. INTRODUCTION

A Wireless sensor network is a network consisting of numerous sensor nodes with sensing, wireless communications and computing capabilities. These sensor nodes are spread in an unattended environment (i.e. sensing field) to sense the physical world. A few sink nodes collect the sensed data through infrastructure networks like the Internet. Sensor networks promise to have a significant commercial impact by providing strategic and timely data to new classes of real-time monitoring applications. One of the most notable challenges looming on the horizon that threatens successful deployment of sensor networks is privacy. Providing privacy in sensor networks is complicated by the fact that sensor networks consist of low-cost radio devices that employ readily available, standardized wireless communication technologies. As a result of the open-architecture of the underlying sensor technology, adversaries will be able to easily gain access to communications between sensor nodes either by purchasing their own low-cost sensor device and running it in a monitor mode, or by employing slightly more sophisticated software radios capable of monitoring a broad array of radio technologies. Through these radio transceivers adversaries may detect the message by interacting with network and trace the appropriate path of data flow in reverse direction to reach to the source.

Hence, this makes us to think about the source location privacy. Preserving the source location means hiding the physical location of the source from the adversaries and increasing difficulty for adversaries in tracing the message path back to the source location. To address source location privacy for sensor networks many of the privacy techniques have been employed. In order to provide efficient and private sensor communications, one of the techniques called phantom routing has proven flexible and capable of protecting the source’s location. Phantom routing approach preserves the actual data packets. In this, source actually sends data to the node called as phantom node which acts as a decoy & then forwards that data to sink node by using the shortest path. But existing routing scheme has phantom node routed to sink directly, adversaries can trace the path back along the route of Phantom node and reach the source. FitfrobRate protocol preserves the source location privacy and also reduces the delay in obtaining data packets.

But all these privacy techniques utilized in general network scenarios are not appropriate for protecting the source location in a sensor network. This is partially due to the fact that many of the methods introduce overhead which is too burdensome for sensor networks. Many techniques lead to increase the packet collision that affects efficiency of packet transmission and also decreases network lifetime.

One of the ideas to preserve source location privacy is to have multiple diversionary routes to the sink. Due to these multiple routes adversaries get confused and face difficulty in reaching the source message. For each diversionary route, multiple Fake nodes are generated. These nodes should have the similar size as that of the source node so that adversaries cannot differentiate between original and fake data packet. But this leads to extra energy consumption which lessens the network lifetime. Therefore, there is need to learn and implement the novel tree based diversionary routing scheme which will help in preserving source location privacy as well as maximizing network Lifetime.

The rest of the paper is organized as follows: section-2 describes the related work and the section-3 concentrates on source location privacy preserving technique. The section-4 describes terminology and section-5 describes Directed Oriented attack along with the solution to overcome that attack to preserve source location privacy.

II. RELATED WORK

1. Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks

The jun lon, mianxiong dong, kaoru ota, and anfeng liu [1] have introduced a innovative tree-based diversionary routing scheme for preserving source location privacy to create diversionary routes along the path to the sink from the real source. They also stated that at the end of each diversionary route a decoy (fake source node), which periodically emits fake events is present.

The authors stated that tree-based diversionary routing scheme is able to maximize the network lifetime of WSNs and the lifetime of WSNs depends on the nodes with is having high energy consumption or hotspot. They have done systematically analyse of the energy consumption in WSNs and provided direction on the number of diversionary routes. These routes can be created in different regions away from the sink. They identified a novel attack against phantom routing namely direction-oriented attack. Moreover they also performed a comprehensive analysis on how the direction-oriented attack can be defeated by the tree-based diversionary routing scheme.

2. On the Use of Fake Sources for Source Location Privacy

Arshad Jhumka, Matthew Leeke and Sambid Shrestha [2] describes the fake source technique in enhancing the source location privacy of wireless sensor networks. The authors have investigated the efficiency of different alternatives of the fake source technique in occurrence of two different implementations of the distributed eavesdropper attacker model.

They stated both the implementations in detail and described that one fake source implementation, FS1, showed poor level of privacy, owing to the very low probability of a node being chosen as a fake source in the network. On the other hand, the FS2 protocol achieved an average, a good level of privacy. An implementation, FS2, when enhanced with two protocol extensions: unique messages and increased rates, achieves nearly perfect privacy level.

The authors have also worked on a novel hybrid technique which is formed from combining fake sources with phantom routing, and show that this hybrid technique provides a nearly perfect privacy level when at least one fake source is present.

3. Enhancing Source-Location Privacy in Sensor Network Routing

The several distinct flooding-based and single-path routing techniques exist but none of these protocols are capable of providing source location privacy. To achieve improved location privacy, the authors Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk [3] proposed a new routing technique called phantom routing, for both the flooding and single-path classes that enhance privacy protection.

The authors stated that in phantom routing the source node send data to the node called phantom node which acts as a decoy & forwards that data to the sink. The goal is to keep the hunter away from the source node. The delivery of every message experiences two phases: random walk phase and single path routing. The purpose of the random walk is to send a message to a random location away from the real source.

The authors made use of generic asset monitoring application called the Panda-Hunter Game as well as refer to a formal model for asset monitoring applications. The game features a hunter in the role of adversary who tries to capture the panda by back-tracking the routing path until it reaches the source. As a result, a privacy routing technique should prevent hunter from locating the source while delivering data to the sink.

4. Maximizing lifetime of event-unobservable wireless sensor

The K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci [4] has observed that, by periodic packet transmission along with dummy traffic filtering at proxy nodes information can be protected against global eavesdroppers. The authors described Linear Programming (LP) framework which was used to analyse lifetime limits of WSNs .Thus preserving event unobservability with different proxy assignment methodologies.

The authors have investigated various proxy assignment strategies and different deployment circumstances. The LP framework is used to characterize network dynamics and energy dissipation. LP framework is modelled with PFS (proxy based filtering scheme) and TFS (tree based filtering scheme). In PFS, data packets pass through a single proxy at most. But in TFS scheme, proxies are organized in tree structure where proxies at higher level combine the packets coming from lower level.

The authors have proposed new scheme called optimal Filtering Scheme (OFS) to maximize the network lifetime in which data flow can pass through multiple proxies.

5. Privacy preservation in wireless sensor networks: A state-of-the-art survey

The Na Li , Nan Zhang , Sajal K. Das , Bhavani Thuraisingham[5] surveyed about the privacy issues in Wireless Sensor Networks. They also provide a state-of-the-art survey of privacy-preserving techniques for WSNs. In particular, t two main categories of privacy-preserving techniques is reviewed. These techniques are used for protecting two types of private information such as data-oriented and context-oriented privacy.

III. SOURCE LOCATION PRIVACY PRESERVING TECHNIQUE

For preserving source node privacy and maximizing network lifetime, one solution is to use Tree based diversionary routing. In Tree based diversionary routing, the phantom node is established away from source. Then routing path is established towards the sink. This tree routing path has multiple diversionary routes as its branches. At the end of these diversionary routes fake source nodes are present which are used to confuse the adversaries while identifying the real source node. The fake source node is called as Decoy.

The main goal of Tree based diversionary routing is to improve performance in two aspects: privacy and network lifetime. In Phantom routing scheme, phantom node sends data to sink by using shortest routing protocol. Hence, adversaries can trace the path in reverse direction and get the location of source node. To overcome this drawback, one solution is to use the Tree based diversionary routing strategy that makes difficult for the adversaries to trace the path of phantom node.

This scheme first establishes the backbone route directed to the network border. Then it establishes multiple diversionary routes which forms branches of backbone route. These diversionary routes are directed towards the network border forming Tree based diversionary routing path. In each diversionary route, data generation and packet length is similar so that high privacy is achieved. As source node generates lots of diversionary routes, adversaries cannot able to find the source location by observing tree routing path.

In order to maximize network lifetime, there is need to reduce the energy consumption in hotspot. Therefore, proposed scheme minimizes energy consumption in hotspot and use huge amount of energy from non-hotspot regions to establish diversionary route which improves network lifetime.

3.1 Tree based diversionary Scheme

The tree based diversionary scheme satisfies tree main principles that preserve the privacy and maximize network lifetime. The three principles are:

i. The established routing trees are homogeneous. As it is homogeneous, adversaries cannot able to find exact location of source by seeing the routing path.
ii. Energy consumption of nodes present in hotspot is not increased. Network lifetime is also not decreased.
iii. The huge amount of energy in non-hotspot region is utilized to create diversionary routes.

The implementation of TR consists of 2 parts:

i. Create a backbone route directed to the network edge which serves principle-1.
ii. Establish diversionary routes to meet principle-2 & 3

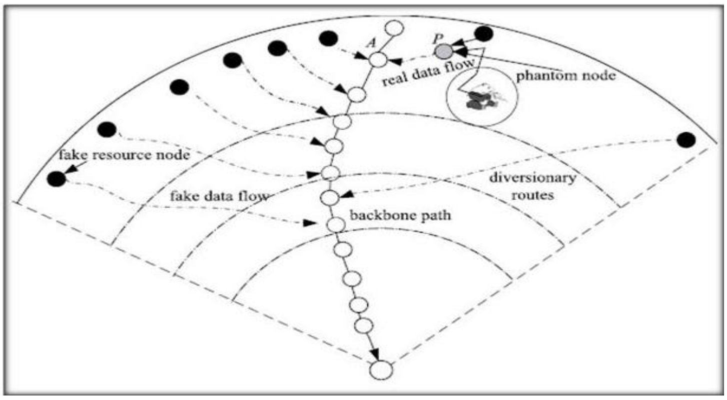

Fig 1 -Tree-based diversionary routing scheme

Fig -1 shows Tree based diversionary scheme in which backbone path is shown from source to the network edge. Multiple diversionary routes are established over the backbone and directed towards network edge. The end of each diversionary route is denoted by Fake node.

3.2 Tree based diversionary routing

This routing scheme consists of three stages: Tree-based diversionary routing establishment, Stable operation stage of the tree-based routing, Destruction of tree-based diversionary routing.

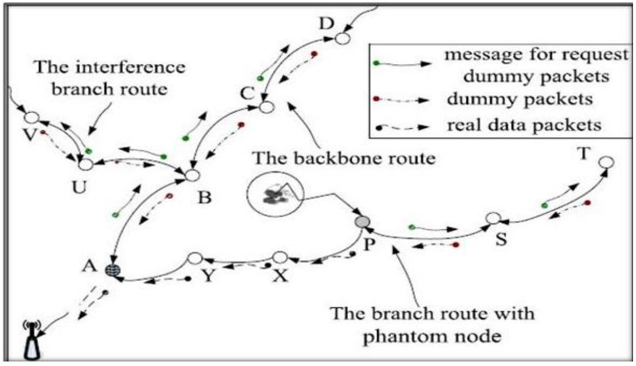

Fig 2- Establishing process of tree route.

3.2.1 Tree-based diversionary routing establishment

i. Tree-based diversionary routing is done by establishing phantom node.

Branch with phantom node is created and then tree trunk is established. As backbone route is easy to trace, phantom cannot remain present on backbone itself. Therefore Phantom node can be on any of the branches. Due to these adversaries faces difficulty in tracing the path of source node.The establishment of Phantom node can be any of the two directions: The Left down direction of Phantom node or the Upper right direction of Phantom node.

If the Left down direction is considered and P is a Phantom node then from figure-2 P selects node X as it is P's neighbor and closest node to the sink. Then X selects node Y having similar hops. Every time node closest to the sink and node with same hop is selected until transmission distance reaches specified hops. Hence node A is intermediate node which is located at specified hops.

If upper right direction of phantom node P is considered then P sends request packet to node S. This packet is contains information as well as frequency of dummy packet. By seeing this node S should send dummy packet to node P in a fixed time interval. In the same way, node S sends request packet to node T. Then T further sends dummy packets to node S. This procedure occurs till network is reached. At the end, branch route is established.

ii. After establishing phantom node, backbone route with intermediate node should be established.

Consider from figure-2 node A is intermediate node. To establish backbone route, there are 2 directions:

- The direction from intermediate node A towards sink
- The opposite direction from A to sink.

iii. Establishing diversionary routes

When a node on backbone wants to establish diversionary route, it sends a request with dummy packets to another node outside the backbone. This node replies back to previous node with dummy packet. Similarly, new node will send a request packet to next node and so on.

From figure-2 node B sends request packet to node U. Node U then sends dummy packet to node B. node U further sends request to node V and so on until it reaches network border.

3.2.2 Stable operation stage of the tree-based routing

When all the nodes are included in the routes, then nodes starts to operate. During transmission, the node sends real data packets if it receives real data packet. If no any real data packet is received then node sends dummy packet in fixed amount of time.

3.2.3 Tree-based diversionary routing Destruction

The destruction of any route in tree depends upon Phantom node P and its intermediate node. When P and node A does not receive any real data packet within fixed amount of time then this routing path will be discarded. Then node P and node A will send the message to other nodes which are present on the same route. Once all the nodes receive stop message instruction then route comes to an end. The nodes on that route will no longer receive any message.

IV. TERMINOLOGY

In TBR scheme, multiple diversionary routes are created. But, these diversionary routes consume lots of energy. Hence, there is need to consider number of diversionary routes and their location in order to maximize network security. Energy is mainly consumed in 2 ways:

i. In creating phantom node

ii. In establishing tree route

Energy is more consumed in establishing tree route. In this, first we will consider the backbone route establishment having no diversionary route. When there is only one backbone route, then network lifetime is the same as that of shortest route algorithm. The backbone present in one ring has highest energy consumption. Even if the path length of backbone is increased, energy consumption still remains constant. Hence, network lifetime remain unchanged.

The diversionary routes are created into other rings. Each ring creates same number of diversionary routes. Therefore, number of diversionary routes which are required in each ring in backbone route is given by:

$$k = \min\left(\frac{2(y-1)m^2 - (2y-1)\varphi}{\sum_{i=2}^{y}(2i-1)}\right) | y \in \{2 \ldots m-1\}$$

The performance indicators used to characterize WSN should be considered. They are:

i. Trace Time: Trace Time defines the safety period which starts from adversaries tracing procedure till it captures the source. The objective of source location privacy is expressed as:

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

If the trace time is max then the source location privacy can be achieved.

ii. Life Time: It defines the period from starting of network operation until the first power outage occurs in WSN. The objective to maximize network lifetime is

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

Where Ei is energy consumption of node I and l is Life time.

The main goal of TR scheme is as follows:

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

V. DIRECTED ORIENTED ATTACK

In phantom route strategy, there exists only one route. This route is from Phantom node to the sink and it is a shortest path. Hence, the route path depends upon the location of Phantom route. Even though phantom node is dynamically selected, adversary can still finds location of source node by adopting effect effective strategy called as Directed Oriented attack.

The main idea of Directed Oriented attack is that it considers distance from Phantom node to sink is just h hops and Phantom path is a shortest path. If the phantom node is uniformly and randomly selected, then Phantom node is generated randomly at distance of h hops from source node. If the adversary collects certain amount of route path information and calculate average direction, then adversaries is able to find out real direction of source node.

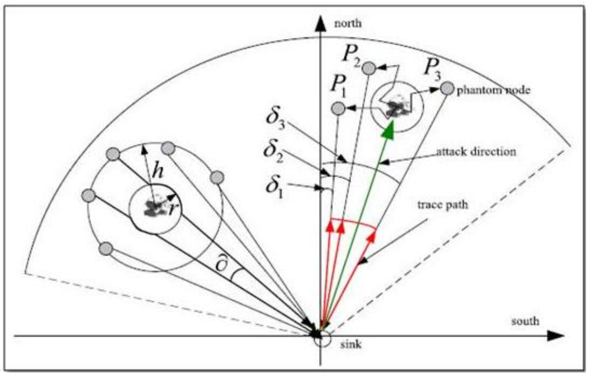

Fig 3- Direction-oriented traces the phantom route.

Consider phantom node p1, p2, p3 as shown in figure.

In order to increase the tracing difficulty for adversaries, these 3 phantom nodes use shorter periods of time. This means that the route is discontinued after shorter period of time. Due to this, adversaries only trace short part of route. But, adversaries think that real source node must be close to these three phantom nodes. For this, adversaries denote the angle between these three paths and Y coordinate. These angles are δ1, δ2, δ3 then adversaries calculate average of these angles such as δ = (δ1, δ2, δ3) / 3. This gives direction to adversaries to trace the path and succeeds in finding source location. The more the directions adversaries know, there is highest possibility that adversaries trace the exact location of source by using average direction.

To avoid direction-oriented attack, the average angle of all backbone routes cannot fall in the visible area. Hence more routes are created in one direction and then the average angle deviates from the visible area. When phantom node is created, the phantom node can decide to create the first branch with the left hand rule or the right hand rule.

Let θ be the probability of choosing left hand rule and h be the maximum distance from the backbone route to the source node, then the average angle is $\overline{X} = -\frac{h}{2}\theta + \frac{h}{2}(1-\theta)$ then we can get

$$-\frac{h}{2}\theta+\frac{h}{2}(1-\theta) > 1 \Rightarrow \theta < \frac{1}{2}-\frac{1}{h}, \text{ or } \theta \geq \frac{1}{2}+\frac{1}{h}$$

VI. CONCLUSION

The source location privacy is a significant issue in Wireless Sensor network. This paper describes the drawbacks of Phantom routing scheme. Although there are various techniques that preserves the privacy of source location, but still there is problem in achieving privacy. One solution to this problem is to use Tree-based Diversionary Routing scheme. In this, diversionary routes are created along the path of source to sink and at the end of each route decoy node is present so that adversaries get confused. This preserves the privacy of source location. Tree-based Diversionary Routing scheme has advantage that route structure is homogeneous so that adversary cannot differentiate between real source node and Phantom node. Tree-based Diversionary Routing scheme provides high resistance over Direction Oriented attack by creating a tree backbone route with left hand rule. Moreover, it helps in maximizing Network Lifetime by reducing energy consumption in hotspot region.

REFERENCES

[1] Long, J., et al. ,"Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks" Access, IEEE 2 (2014): 633-651.

[2] Jhumka, Arshad, Matthew Leeke, and Sambid Shrestha, "On the use of fake sources for source location privacy: trade-offs between energy and privacy" The Computer Journal 54.6 (2011): 860-874.

[3] Kamat, Pandurang, et al., "Enhancing source-location privacy in sensor network routing" Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on. IEEE, 2005.

[4] Bicakci, Kemal, et al. "Maximizing lifetime of event-unobservable wireless sensor networks" Computer Standards & Interfaces 33.4 (2011): 401-410.

[5] Li, Na, et al., "Privacy preservation in wireless sensor networks: A state-of-the-art survey" Ad Hoc Networks 7.8 (2009): 1501-1514.

[6] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey" Computer networks 38.4 (2002): 393-422.

[7] Chen, Honglong, and Wei Lou. "From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks." Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International. IEEE, 2010.

[8]Mahmoud, Mohamed MEA, and Xuemin Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks" Parallel and Distributed Systems, IEEE Transactions on 23.10 (2012): 1805-1818.

[9] Ozturk, Celal, Yanyong Zhang, and Wade Trappe, "Source-location privacy in energy-constrained sensor network routing" SASN. Vol. 4. 2004.

[10] Li, Yun, and Jian Ren, "Preserving source-location privacy in wireless sensor networks" Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on. IEEE, 2009.

[11] Wang, Haodong, Bo Sheng, and Qun Li. "Privacy-aware routing in sensor networks" Computer Networks 53.9 (2009): 1512-1529.

[12] Mehta, Kiran, Donggang Liu, and Matthew Wright, "Location privacy in sensor networks against a global eavesdropper" Network Protocols, 2007. ICNP 2007. IEEE International Conference on. IEEE, 2007.

[13] Tan, Guangbao, Wei Li, and Jie Song, "Enhancing Source Location Privacy in Energy-Constrained Wireless Sensor Networks" Proceedings of International Conference on Computer Science and Information Technology. Springer India, 2014.

[14] Ouyang, Yi, et al, "Entrapping adversaries for source protection in sensor networks" Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks. IEEE Computer Society, 2006.