# Research on Location Privacy Protection Methods of Wireless Sensor Network in Smart Grid

Hua Ye
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: huaye@sgri.sgcc.com.cn

Huang Xiuli
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: huangxiuli@sgri.sgcc.com.cn

Zhang Tao
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: zhangtao@sgri.sgcc.com.cn

Ma Yuanyuan
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: mayuanyuan@sgri.sgcc.com.cn

**Abstract — With the development of electric power, communication, network and sensor technology, the applications of wireless sensor network in smart grid will be more extensive. However, the privacy issues of wireless sensor network will also be more obvious with variety of applications, if we do not take appropriate measures to protect the privacy of the network, network security and availability will be greatly reduced. This article discussed the location privacy protection issues of wireless sensor networks in smart grid. Firstly, we gave a brief introduction to the concept of wireless sensor network and its application in the smart grid, and we pointed out the privacy issues of wireless sensor network. Secondly, we described location privacy protection issues in wireless sensor network, and then we gave the attacker models. Thirdly, we described several location privacy protection technologies of source nodes and sink nodes, and their performance was analyzed and compared. Finally, we gave some suggestions on the concern in location privacy preservation technologies of wireless sensor network in smart grid. This study shows that existing location privacy protection methods can protect location privacy of key nodes at a certain degree, but they can not completely make the network to meet low energy consumption, long safety time, low latency and high packet receiving rate. How to design a more efficient location privacy protection method is the focus issue in future research.**

***Keywords-smart grid; wireless sensor network; node; location privacy protection; security.***

## I. INTRODUCTION

Wireless sensor network uses a large number of miniaturized sensors distributed in the area to be monitored, each sensor is used as a node, these nodes communicate via electromagnetic signals, they form a multi-hop, self-organizing network [1]. Wireless sensor network nodes collaborate to perceive the objects which be monitored in network coverage area, collect and process related data and send them to observers. Wireless sensor network has characteristics with large-scale, self-organizing, multi-hop routing, dynamic, resource-constrained, data-centric and application-related. Now, wireless sensor network has been widely used in military, environmental monitoring, medical, industrial control and other fields [2].

In smart grid, wireless sensor network has also been used in many ways, such as remote meter reading, substation automation, distribution network protection, distribution line fault locator, online monitoring of transmission lines [3]. Among them, online monitoring of transmission lines is a typical application in smart grid. Online monitoring of transmission lines is mainly used to monitor the operation status of EHV transmission lines and diagnose the status of transmission lines devices. The system uses a variety of sensors to detect the status of transmission lines and their environment, such as: temperature, humidity, wind direction, wind speed, filthy, icing conditions, stress conditions, the video images. The system does line fault detection and management in the multi-information integration and fusion conditions. By deploying wireless sensor network nodes in transmission lines and deploying gateways in the tower, it is available for large span transmission lines condition monitoring.

With the increase in the field of wireless sensor network applications, privacy issues in network are becoming increasingly clear. Privacy threats directly affect the deployment and application of wireless sensor network, it has been widespread concern. Privacy protection has been studied extensively in several areas such as: database, wired network, wireless network and data mining and so on. But in wireless network, uncontrollable environment, constrained node resource and confined topology are the challenges to privacy protection, research is still in its infancy, there are many

issues to be resolved. Privacy protection of wireless sensor network mainly involves three aspects: data privacy protection, location privacy protection and identity privacy protection. Among them, the main task of location privacy protection is to protect the key nodes in network, prevent attackers learn their physical location and attack them. In online monitoring of transmission lines, it's very necessary to protect location privacy of key nodes, it's a prerequisite for making the whole system work effectively and lines stability and safe operation.

## II. LOCATION PRIVACY PROTECTION OF WIRELESS SENSOR NETWORK

In wireless sensor network, we should protect location privacy of key nodes, prevent attackers from attacking against these nodes. Key nodes have important position in the network, they bear more responsibility than the other nodes. Once the location of key nodes be known by attackers, the attackers can attack them, causing great damage to the network. Wireless sensor network location privacy protection is primarily aimed at the source node and the sink node [4].

### *A. Location privacy protection of source node*

The source node is used to collect information of objects to be monitored, and spread information data in internet, at last send it to the sink node. The source node is usually the node which closest to the object be monitored, once the location of the source node is found, it will directly lead to exposure of the object be monitored. Data collected by the source node will be sent to the sink node, this is bound to form one or more paths from the source node to the sink node, external attackers can find the location of source node by tracing packet. Completely avoid the attackers eavesdropping data, tracing the location of the source node is impossible, currently, the research of source node location privacy protection focuses on how to extend the time that attackers traces the source node, provide better security performance for the network.

### *B. Location privacy protection of sink node*

As the source node, sink node is also a key node in the wireless sensor network. Sink node is a gateway for wireless sensor network and external network connection, data collected by source node will be sent to observer through sink node, meanwhile, the sink node is also responsible for publishing the entire network detection tasks. If the location of sink node be obtained by an attacker, and then be destroyed, it will result in paralysis of the entire network. Since the data packet usually be sent to the sink node from the source node follow some routing paths, traffic patterns of network will exhibit the phenomenon of unequal, the closer to the sink node, the greater the traffic of data, data flow nearby the sink node is the greatest in the whole network, an attacker can easily obtain the location of the sink node by traffic analysis method.

### *C. Attacker model*

Attackers in wireless sensor network location privacy issues are divided into two groups: external attackers and internal attackers. Internal attackers mastered packet exchange format and semantic, they can crack contents of the packet transmitted in the network. External attackers don't need to crack contents of the packet, just by listening to the network traffic, they can obtain location privacy according to whether there have data flow in network, the size of the data flow and the signal source. Internal attack is more difficult, and external attack is relatively easier. Currently, the attackers which attack against the location privacy of wireless sensor network is almost external attackers, attackers are divided into attackers tracing packet transmission hop by hop (local attackers) and traffic analysis attackers(global attackers). In this paper, we consider the situation of location privacy protection against external attackers.

*1) Attackers tracing location of source node hop by hop*

Attackers use wireless signal positioning device to monitor packet transmission behavior within a certain range, listening range is usually one hop transmission range, it traces the location of the source node by the data packet transmission with the opposite direction. First, the attacker stays in the vicinity of the sink node, and monitors the wireless signal within a local region, when a new signal is detected, the attacker will infer the location of the signal transmitting node, then it will move to this node to continue listening, finally, it will trace the location of the source node by using hope by hop way. Figure 1 depicts the process that an attacker tracing location of source node hop by hop.

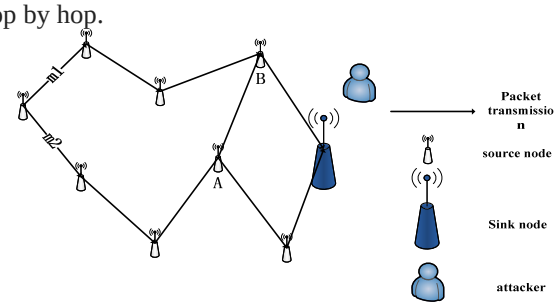


Figure 1. Backtracking source node

*2) Attackers tracing location of sink node hop by hop*

When the attacker in such way to trace the location of the sink node, it infers the node on the transmission path according to the time sequence of the data packets be sent, then it moves to the sink node hop by hop. Figure 2 depicts the process that an attacker tracing location of sink node hop by hop.

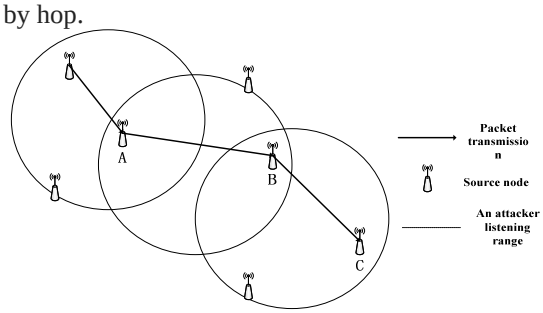


Figure 2. Tracking sink node hop by hop

*3) Traffic analysis attackers*

The traffic analysis attackers can monitor wireless communication within the whole network, they always have high attack capability. Attackers use a large number of low-cost monitoring equipment in network for global monitoring, by observing and analyzing network traffic patterns, attackers can locate the position of the source node or sink node.

## III. WIRELESS SENSOR NETWORK LOCATION PRIVACY PROTECTION TECHNOLOGIES

At present, the location privacy protection strategies can be divided into three categories: random routing strategy, garbage bag strategy and camouflage strategy. In random routing strategy, every time a packet is sent, it's not transmitted from the source node to the sink node direction, but is transmitted to a direction away from the sink node with a certain probability, and randomly generated for each data packet transmission path. Since this process increases the length of the transmission path, the attackers must wait a long time to listen to the wireless signals and continue tracing, the security time of network is extended; the main idea of garbage bag strategy is to produce some garbage bags in the network, by confusing the attackers, making attackers can not properly distinguish between data packets and garbage bags, attackers will be introduced into the wrong position, extends the follow-up time; camouflage strategy by placing some dummy nodes which have the capable of simulating the protected nodes in the network, it will guide the attacker to a wrong location that away from the true target.

In table 1, it shows some typical techniques of source node location privacy protection and sink node location privacy protection, the performance of the technology will be evaluated and compared. We chose the following four indicators to evaluate the performance of various location privacy protection methods: the degree of privacy protection, accuracy, latency, the extra energy consumption. Wherein the accuracy includes the following two aspects: (1) the accuracy that sink node receives data, (2) the possibility that the data successfully transmitted to sink node, latency include the computing and communication time when the intermediate node transmits data, the extra energy consumption refers to the additional energy consumption brought by the method used to protect the privacy of wireless sensor network.

Table 1. analysis of the performance of the wireless sensor network location privacy protection methods

| **Location privacy protection methods** | **the degree of privacy protection** | **accuracy** | **latency** | **the extra energy consumption** |
|---|---|---|---|---|
| Flooding(for source node) | For baseline flooding: it can easily find the shortest path between the source node and the sink node.<br>For probability flooding: probability depends on the previously set. | For baseline flooding: to ensure that data reaches the base station.<br>For probability flooding: it can not guarantee that the data reach the base station. | For probability flooding: the data is not guaranteed to be transmitted on the shortest path. | Additional energy consumption is mainly in full online flooding. |
| Random routing [7](for source node) | The attacker is not easy to find the true source node. | For Phantom routing: all the data can reach the base station.<br>For greedy random forwarding: arrival data is dependent on the intersection of two paths. | For phantom routing: depends on the number of hops of random forwarding.<br>For greedy random forwarding: it relies on randomness. | Additional energy consumption is mainly in random forwarding. |
| Loop trap routing protocol(for source node) | It can make the attackers run into the wrong path, and extends the time that they traces the source node. | No effect on the accuracy and arrival of the data. | It delays arrival of true data, so that the transmission rate is consistent with dummy packet transmission rate. | Additional energy consumption is mainly in injection and transmission of dummy packets. |
| Dummy source node strategy(for source node) | It makes the attacker's attention away from the true source node. | No effect on the accuracy and arrival of the data. | No additional latency. | Additional energy consumption is mainly in dummy data that produced by dummy source node. |
| Re-encryption strategy [8](for sink node) | Re-encrypting the data changes the appearance of the packet for the sink node location privacy protection. | No effect on the accuracy and arrival of the data. | Data encryption and decryption of intermediate nodes takes time. | No additional energy consumption. |
| Multi-parent node routing(for sink node) | Using multiple route paths for data transmission. | No effect on the accuracy and arrival of the data. | No additional latency. | No additional energy consumption. |
| Dummy sink node(for sink node) | Using multiple dummy sink nodes to share the traffic of true node, making the attacker can not determine the location of the real sink node. | Attackers attacking the dummy sink node may cause loss of same data. | No additional latency. | Data fusion of dummy sink node will bring energy consumption. |
| Random Routing [9](for sink node) | Depends on the probability of selecting a parent node as the next hop. | There is no guarantee for data arrival, it depends on the chosen probability. | Depends on the selected next hop. | Additional energy consumption is mainly in random forwarding. |
| Location protection routing protocol(for sink node) | An attacker can not determine whether the next hop is closer to the sink, and it may be brought to the wrong direction by garbage bag. | No effect on the accuracy and arrival of the data. | Depends on the selected next hop. | Additional energy consumption is mainly in randomly selecting next hop and producing garbage bag. |
| Differential branch routing protocol(for sink node) | Using random packet forwarding and garbage bag strategy can defense the attackers tracing hop by hop and traffic analysis attackers. | No effect on the accuracy and arrival of the data. | Depends on the selected next hop. | Additional energy consumption is mainly in randomly selecting next hop and producing garbage bag. |
| Randomly selected transmission time [10](for sink node) | Making ambiguous relationship of parent and child nodes. | No effect on the accuracy and arrival of the data. | Randomly selecting transmission time in each time segment. | Need to consume less energy for synchronization control of time segment. |

## IV. WIRELESS SENSOR NETWORK PRIVACY PROTECTION IN SMART GRID

A typical application of wireless sensor network in smart gird is online monitoring of transmission lines [5]. In the system of online monitoring of transmission lines, the source node of wireless sensor network is responsible for collecting various data on lines, and the data is sent to the sink node via multi-hop network. If the location of source node is found by the attackers, the attackers may attack the node, failure of the node will result in the network can not access the status of the lines that be monitored timely and accurately, the system can not make emergency treatment on the line fault. Sink node is a gateway to connect a wireless sensor network and external network, it is responsible for data analysis and integration, and sends data to the administrator. The destroy or isolation of sink node will cause failure of the entire network which result in loss of effective monitoring of online monitoring system. So it is important for source node location privacy protection and sink node location privacy protection in wireless sensor network in the online monitoring of transmission lines system.

By analyzing and comparing location privacy protection technologies mentioned in this paper, it can be seen that: (1) different location privacy protection technologies have played a key role in protecting the location privacy of key nodes and extended the security time of the network, but the effect of location privacy protection of different techniques is different from each other, (2) the use of certain technologies may extend the processing time that sink node receives data, even the sink node can not successfully receive data, (3) the main consideration for wireless sensor network on location privacy protection is the energy consumption, most methods require additional energy consumption.

It must be considered in online monitoring of transmission lines that: (1) location privacy of source node and sink node is effectively protected, (2) sink node must be able to successfully receive the monitored data of lines, (3) the monitored data of lines must be received by sink node within the specified time, (4) the additional energy consumption of the entire wireless sensor network should not be too large to ensure the life cycle of the network. Therefore, the choice of location privacy protection method must be considered, for example: for the source node location privacy protection, we can choose dummy source node strategy, for the sink location privacy protection, location protection routing protocol and differential branch routing protocol will be a good choice.

Location privacy in wireless sensor network is just in a starting stage, there are many issues to be resolved, for example: how to reduce the energy consumption of the network, how to get more safety time for the network, how to protect the location privacy for dynamic node and so on. Combining application of wireless sensor network in smart grid, the next step of the research is to design a wireless sensor network privacy protection method with low energy consumption, long safety time, low latency and high packet receiving rate combine with the existing location privacy protection technologies.

## V. CONCLUSION

With the development of electric power, communication, network and sensor technology, the applications of wireless sensor network in smart grid will be more extensive [6]. However, the privacy issues of wireless sensor network will also be more obvious with variety of applications, if you do not take appropriate measures to protect the privacy of the network, network security and availability will be greatly reduced. Location privacy of wireless sensor network is an important privacy, the exposure of location privacy of source node will directly expose the object to be monitored, the destruction of the source node will lead to the result that the network can not collect data here, sink node is a gateway between wireless sensor network and external network, also it is responsible for the collection and integration of data sent from the source node and transmitting it to the administrators, destruction and isolation the sink node can lead to paralysis of the network, so it is necessary to protect the location privacy of source node and sink node. Existing location privacy protection methods can protect location privacy of key nodes at a certain degree, but they can not completely make the network to meet low energy consumption, long safety time, low latency and high packet receiving rate. In the location privacy protection methods of wireless sensor network in smart grid, the next step in the research is to design some more effective location privacy protection methods that meet the requirements of location privacy protection of wireless sensor network in smart grid.

## REFERENCES


[1] Zhao Baokang. Key technologies for wireless sensor networks privacy protection[D]. Changsha: National University of Defense Technology, 2009.

[2] Liu Minyue, Wu Yong, Wu Weiguo. Wireless sensor networks WSN Research[J]. Jilin Electric Power, 2010,38（2）：20-23.

[3] Zhang Qiang, Sun Yugen, Yang Ting, Cui Zhenhui. Wireless sensor network applications in the smart grid[J]. China Power. 2010,43（6）：31-36.

[4] Wang Sheng. Research on wireless sensor network location privacy protection[D]. Changsha: Central South University, 2009.

[5] Lan Shaoping, Chen Jianbin, Zhu Hangjie. Wireless sensor network application prospects in the smart grid[J]. Information Engineering, 2014,12 : 42.

[6] Dong Hao. Research on Application of wireless sensor networks in smart grid[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2013.

[7] Y. Xi, L. Schwiebert, W.S. Shi, Preserving source location privacy in monitoring-based wireless sensor networks, in: Proceedings of the20th International Parallel and Distributed Processing Symposium (IPDPS 2006), April 2006.

[8] Li Na, Zhang Nan, Sajal K. Das, Bhavani Thuraisingham, Privacy preservation in wireless sensor networks: A state-of-the-art survey, Ad Hoc Networks 7 (2009) 1501-1514.

[9] Y. Jian, S.G. Chen, Z. Zhang, L. Zhang, Protecting receiver-location privacy in wireless sensor networks, in: Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM2007), May 2007, pp. 1955–1963.

[10] J. Deng, R. Han, S. Mishra, Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks, Pervasive and Mobile Computing Elsevier 2 (2) (2006) 159–186.