HPCT:A Novel Scheme for Protecting Source-Location Privacy in WSN

Guanghui Chang[1, a], Laijun Li[2, b], and Guangxia Xu[3, 1, c]

[1]School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China;

[2] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China;

[3] The Information and Communication Engineering Postdoctoral Research Station, Chongqing University, Chongqing 400044, China.

[a]Changgh@cqupt.edu.cn, [b]metalage@126.com, [c]xugx@cqupt.edu.cn

Keywords: Hash encryption, compromise node, global eavesdropping, periodic collection, source anonymous.

Abstract. In wireless sensor networks (WSNs), although there are many existed schemes for the local eavesdropper. However, a global eavesdropper who is well-equipped, highly motivated and has the ability to compromise node can make those method invalid, so that those existing techniques can't be against such attacks. In this paper, we proposed the Hash Periodic Collection technology (HPCT) through applying the hash encryption to the PCT for the purpose of protecting the location privacy of the source node under the global eavesdropping attacks and compromised node attacks. The experiment showed that the Hash Periodic Collection technology (HPCT) we introduced is better than PCT, and the HPCT dramatically increased the security and safety time of the source location privacy.

Introduction

The internet of things is the third wave of the world information industry after computer, internet and mobile communication network [1]. With the development of the internet of things, the wireless sensor networks have great prospects of developing as an indispensable part of the internet of things [2]. WSN is a self-organizing network that is mainly composed of a number of multifunction sensors, which have the characteristics of low cost, small size and limited resources. It is always used in the place inconvenient to establish a wired network, and can be exploited to monitor physical world [3].

In WSN, in spite of the content of the packet having been encrypted, the location privacy remains a serious threat, especially in the hostile environment. Due to the openness of wireless sensor networks, the packet information can be easily eavesdropped by enemy. Then the monitored information (packet transmission time and frequency) may be used to perform traffic analysis attacks to estimate the physical location of the object. However, the traditional anonymity techniques (Random routing [4], inject garbage packets [5], etc.) are not only very expensive but also can't protect the location privacy well of the node.

Related Work

In this section, we describe some methods which have been proposed to protect the source location privacy, and was designed to protect the reality of the object from the local eavesdroppers through increasing safety time. Safety time: the number of packets has been sent by source node before it was positioned.

Kamat et al. describes the phantom single-path routing [7]. It is divided into two stages - the random walk phase and single-path routing phase. To avoid random walk cancelling each other out, it is divided based on the number of hops and quadrant. The general process of the phantom single-path routing is: first, the packet of source node sent reach to some arbitrary node after H hops through random walk. Second, utilize the single-path routing to reach the sink.

Flooding technology [6]. The source node may send packets to the sink through many different paths in order to achieve the purpose of confusing the attacker. But the base station receiving the packet from the shortest path still is the very first, so the attacker also can capture the location information of source node very quickly. Due to the generation of a lot of paths, this method can not only consume a lot of energy, but does not reach the high level of privacy.

Cyclic entrapment method [8]. Different places in wireless sensor networks generate multiple cycle paths to fool the enemy into the repetitive cycle path, thus increasing the safety of the time, and making the source node be well protected. Energy consumption and the level of location privacy will increase with the increase of the circulation path.

Network and Attack Model

Network Model. In this paper, the wireless sensor network consists of a sink and many other ordinary nodes, they are some of the cheap, small, limited energy, low processing speed and storage capacity of the sensor [9], where the sink as the only gateway, its performances in all aspects are better than the ordinary node. The equipment is mainly used in various monitoring areas such as wildlife habitat, buildings or military applications, and so on. We consider it as a homogeneous network model. In this homogeneous network, in addition to the sink, all of the other nodes have almost the same computing power, energy and life cycle. They are uniformly distributed in a certain area. The sink is a credible and strong data receiving device, which is responsible for collecting sensor data from other nodes.

Attack Model. In the wireless sensor network, we assume that there is a high mobility and well-equipped, and the attacker has the ability of compromise node, its main purpose is to obtain sensitive information from monitored object. In this paper, we consider the attacker is a global listener who has the ability to compromise node. For a high motivated attacker, tapping the entire wireless sensor network is an efficient and fast way to locate the objects of monitored. For the attacker, there are two practical ways to achieve this goal. First, configure his eavesdropping network to target wireless sensor network. Second, place a small number of strong powerful nodes to eavesdrop the entire network. However, since the wireless transmission radius of the node has limitation, so the deployment density of the node needs to be large enough to sense the wireless signal from all the sensor nodes. In fact, the second configuration is more expensive in real life, in order to listen to the entire network, we can’t reduce the nodes those battery are powerful. Therefore, we consider the first configuration mode in this paper is more realistic.

Privacy Protection Routing

In this section, we propose a hash periodic collection technique based on the one-way hash chain in the basis of the paper which can only provide protection for the location privacy under a attack of global eavesdrop. In addition, we assume that the content of communications between two sensor nodes is encrypted, so that even if attackers intercept data packets, it only can compare two packets while can’t determine the content of the packet.

One-way Hash Chain. In wireless sensor networks, the header of each sending data packet has a special ID number corresponding to the physical address of the node, it’s a direct threaten to the source node location privacy if an attacker intercepts the packets and gets the ID value, what we have to do is to use an one-way hash chain to hide the ID. One-way hash chain is a series of hash values generated by one-way hash function [10]. And the basic idea as follows: using a unique hash function which is valid for all the source nodes to generate a one-way hash chain to identify the source node. Packet structure shown in Table 1:

Table1. The format of packet

DstID	SrcID hash	Rehash seed	Payload Length	Payload	Filter

The parameters are described below:

a) *DstID*: The destination ID of the packets to be sent.

b) *SrcID hash*: Unique hash source ID for identification at the sink.

c) *Rehash seed*: The seed for regenerate a one-way hash chain.

d) *Payload Length*: The content length of the packet.

e) *Payload*: the actual data of the packet, which contain the time of the event occurred and duration. Meanwhile, the data will be encrypted with the symmetric key that shared between source node and sink.

f) *Filler*: It is used to provide a standard length of packets which can be randomly filled with garbage data.

In the pre-configuration phase, each node has its own unique initialize ID and a hash function and a re-hash function. At the same time, the sink will generate a one-way hash chain for each node. For example, the one-way hash chain of node i is $\{h_i^1, h_i^2, h_i^3, \ldots, h_i^i, \ldots, h_i^n\}$, as shown in Figure 1

.

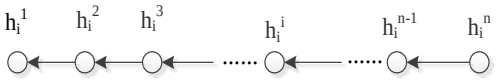


Fig. 1. The one-way hash chain

Then, the sink will send the pre-established one-way hash chain to every node in the form of broadcast. Note that each node will use the one-way hash chain in reverse direction. That is to say, the node i use $\{h_i^1, h_i^2, h_i^3, \ldots, h_i^i, \ldots, h_i^n\}$ in turn as the new packet's ID when sending message. In addition, by the nature of the one-way hash function, we can know that it is basic impossible to calculate the h_i^{i+1} use h_i^i. The same source node will carry different ID numbers when it sends different packets after the one-way hash chain has been generated, so that it will achieve the effect of confusing the enemies. A rehash seed will be sent to one node by sink when the hash ID of the node almost exhausted (less than 10%). After that, the node regenerates the one-way hash chain for itself.

Hash Periodic Collection Technique. In this section, we introduce a new and improved technology HPCT (combined hash function with periodic collection technique) to protect the position privacy and the security of the node in the global eavesdropping attack model which has the ability to compromise node. Among them, although the periodic collection technology (PCT) can achieve the best level of privacy in a global listener, it can only be used for low-rate data collection and data transmission delay which is not strictly required applications [11]. It can't protect the source node's location privacy under the compromise node attack. Just as described in the second part, many outdated methods can't protect the source node's location privacy under the global eavesdropping. The main reason is that a real object existence will change its traffic patterns, which allow global eavesdropper easily find its place. Generally speaking, we can solve this problem as long as traffic patterns and real object are independent. To solve this problem, we proposed a solution as follows:

STEP1: In the pre-configuration stage, defines the format of the data packets sent by each node as shown in Table 1. In order to make the source node anonymous, the one-way hash chain $\{h_i^1, h_i^2, h_i^3, \ldots, h_i^i, \ldots, h_i^n\}$ was joined in the packet header by us. In particular, each sensor node has a timer to trigger an event every *e* seconds, no matter there is real data packets need to be sent.

STEP2: The node send the cache data in the way of FIFO, and the length of FIFO sequence is q which carry real data. When the timer starts, the node will check whether there is a packet to be sent from the sequence. Remove it in accordance with the FIFO principle if it does, then encrypt it by using symmetric key ($Y = sk(\text{Message})$) shared with the destination node, and ready to forward it to the destination node at last. The destination node can use the shared secret key to decrypt the message($Message = sk(\text{Y})$). Otherwise, generate a virtual packet with random load and ready to forward it to the destination node.

STEP3: The sink broadcast a data packet with a hop count counter to the whole network. Then, each node can know the hops between itself and sink. Thus, a neighbor node set S_n is established for each node. The hops of the node in the neighbor node set are smaller than the node itself to the sink.

It is for this reason, the packets can be always transmitted toward the sink and select irregular next hop to confuse the enemy. Finally, the source node randomly select a node from the neighbor set and send the data packet to it.

STEP4: After the first two steps, the packet was sent to the next hop. If the data packet has not been used public key mechanism or the buffer sequence is full, the packet will be dropped. Because of the data packet has not been used public key mechanism, so the packet is considered a garbage packets and discarded. On the other hand, the packet will be accepted.

STEP5: Determine whether the node is a sink? The data packets are successfully transmitted if it is. Otherwise, repeat operation from STEP2.

Simulation and Evaluation

In this section, we use OMNET and MATLAB conduct the simulation in terms of energy consumption and safety time of node. And use the performance of these two aspects to evaluate our proposed method.

In this simulation, we introduce a classic panda-Hunter model [7], and use the terms of it to describe our simulation. In our simulations, including 101 nodes, are randomly distributed in the square area of 100 × 100 m^2 to monitor panda, which sink is used to receive all the real data coming from other nodes, and the location coordinates is (50, 0). The radius between node and node is 50m and each node has a nearest-neighbor node set of 18 [6,7]. The emit radius of RFID tags on pandas is 25m. As shown in Figure 2 is node distribution graphic in our sensor network.

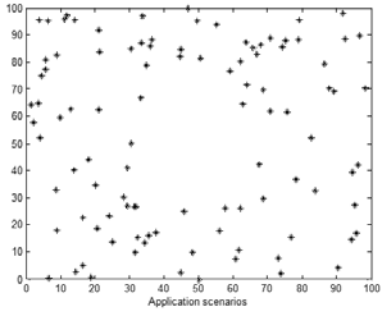


Fig. 2. The node distribution graphic in WSN

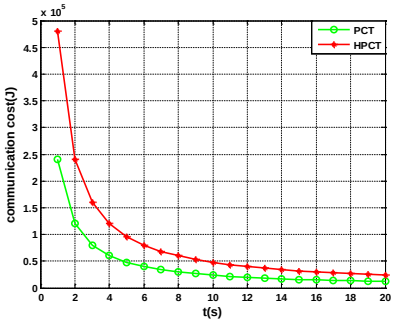


Fig. 3. Energy Consumption

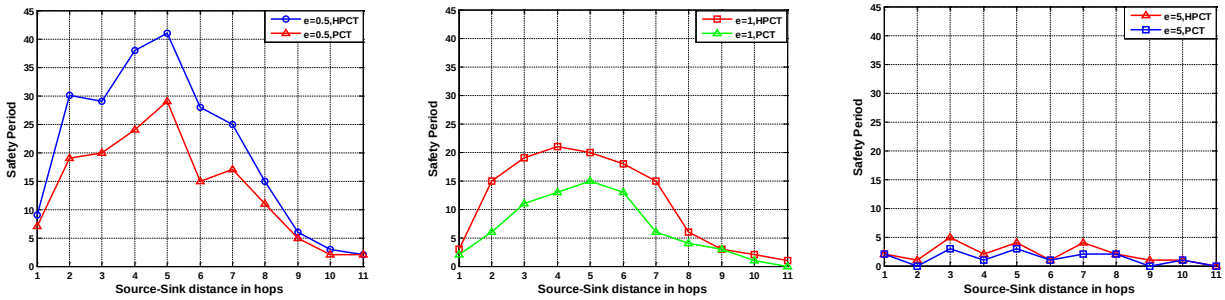
As part IV Analysis, the periodic collection method has reached the optimum location privacy without the attacker who can't compromise node, and the number of monitored object and its movement pattern are independent of the communication energy consumption in the wireless sensor networks. But, periodic collection method is based on a certain time interval to send packets, and with the different frequency of sending packet will affect the communication energy consumption and safety time. Therefore, our simulation focus on analyzing the communication energy consumption and safety time under the attack of compromise node and different frequency of sending packet in the sensor network.

As shown in Figure 3, it depicts communication energy consumption between PCT and HPCT under different time interval of sending packet. With the time interval increasing, the communication energy consumption of PCT and HPCT is continues decreased. This is because the use of periodic collection technique, regardless of whether the actual data to be transferred, it must follow certain frequency of sending packet to send a packet, so as to ensure the source node's location privacy in the global attack. Thus the larger the time interval, the less data packets transmitted within 10min of the simulation time, and the energy consumption will be reduced. From Figure 3, we can also see that the energy consumption of HPCT is always larger than the PCT, which is due to the HPCT have to protect node's location privacy under the attack of compromise node, thus add a hash encryption in the packet header to ensure the anonymity of the data source in order to achieve the effect of confusing the enemy. In other words, the source node can't be found. Although compared to the

energy consumption of the PCT, HPCT slight increase in energy consumption. However, a slight increase in energy consumption can be accepted while compared to its increase of safety time.

As shown in Figure 4-a to 4-c, the safety time of PCT and HPCT is variously based on the different hops between source node and sink within simulation time T. We can see that HPCT's safety time is larger than PCT at the same time interval e. The PCT can't deal with the attacker who has the ability of compromising node which may serve as the reason. On the contrary, the HPCT's safety time is higher because in its packet header the one-way hash chain has been added, thus ensuring the anonymity of the source node, even if an attacker compromise a node can't know the location of the source node, the attack fails. We also found from the figure, with the increase of the time interval e, the safety time of PCT and HPCT subsequently reduced. This is due to the time interval increase, so that the packets of source node which have been sent are reduced and the packets of sink received are reduced also, thereby reducing the safety time. As can be seen from Figure 4-b and 4-c, the gap of PCT and HPCT's safety time is not so big when the time interval is increased sufficiently large.

In summary, the communication energy consumption and safety time will change with the different frequency of sending packet. Although a slight increase in energy consumption, the most important thing is that HPCT greatly improves the safety time after mix in hash encryption. And it's very good to resist the attack of node compromise.



a. safety time (e=0.5s) b. safety time (e=1s) c. safety time (e=5s)

Fig. 4. Safety period

Conclusion

In spite that HPCT still can protect the location privacy safety of source node under a global eavesdropper with node compromise attack model. However, its energy consumption is relatively high because of it must continue send data packets no matter whether there is the real data packet within total run time T. At the same time, each node send the buffered data packets are in accordance with the FIFO principle, so the latency is very large. Therefore, in future work, how to reduce the energy consumption and how to reduce the delay are quite challenging and worthwhile research directions.

Acknowledgement

The authors acknowledge support from the Project Foundation of Chongqing Municipal Education Committee (No. KJ1500441), the National Natural Science Foundation (No. 61309032, No. 61272400), China Postdoctoral Fund (No. 2014M562282), the Project Postdoctoral Supported in Chongqing (No. Xm2014039), Collaborative Innovation Center for Information Communication Technology (No. 002), the Comprehensive Technology Application Demonstrated Project of Safety Smart City in Nan'an District of Chongqing city (No. 2013GS500303-Y3), Research on Intelligent Big Data Analysis and Process Technology for Business Intelligent(No. A2015-44).

References

[1] Perera C, Zaslavsky A, Christen P, et al. Context aware computing for the internet of things: A survey [J]. Communications Surveys & Tutorials, IEEE, 2014, 16(1): 414-454.

[2] Bokare M M, Ralegaonkar M A. Wireless Sensor Network [J]. International Journal of Computer Engineering Science (IJCES), 2012, 2(3).

[3] Lara R, Benitez D, Caamano A, et al. On Real-Time Performance Evaluation of Volcano-Monitoring Systems with Wireless Sensor Networks [J]. IEEE Sensors Journal, 2015, 15:3514-3523.

[4] P. W. Wang, L. Chen, X. J. Wang, A source-location privacy protocol in WSN based on locational angel// Proceedings of the IEEE International Conference on Communications (ICC). Beijing, China, 2008, pp.1630-1634.

[5] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, towards event source unobservability with minimum network traffic in sensor networks. In Proceedings of the first ACM conference on Wireless network security, 2008, pp. 77-88.

[6] C. Ozturk, Y. Zhang, and W. Trappe, “Source-Location Privacy in Energy-Constrained Sensor Network Routing”, Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN ’04), Oct. 2004.

[7] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, Enhancing source-location privacy in sensor network routing. In Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on (pp. 599-608). IEEE.

[8] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, Entrapping adversaries for source protection in sensor networks. In Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks (pp. 23-34). IEEE Computer Society.

[9] Yu H, He J, Zhang T, et al., Enabling end-to-end secure communication between wireless sensor networks and the Internet [J]. World Wide Web-internet & Web Information Systems, 2013, 16(4):515-540. S. Sivashankari and R.M, A framework of location privacy and minimum average communication under the global eaves dropper.2013, IEEE. pp. 392 - 395.

[10] Z. Tao, Y. Liu, C. Li, Strategy of source-location privacy preservation in WSNs based on phantom single-path routing. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2013, pp.178-183.

[11] K. Mehta, D. Liu. M. Wright, Location privacy in sensor networks against a global eavesdropper[C]. Proceedings of the IEEE International Conference on Network Protocols, Beijing, China, 2007, pp.314-323.