Network Working Group
Internet-Draft
Expires: November 29, 2014
L. Zhou
J. Huang
SouthEast University
May 28, 2014

The Location Privacy of Wireless Sensor Networks: Attacks and Countermeasures
draft-zhou-rrg-lp-wsn-00

Abstract

With the related applications of wireless sensor networks getting into our lives quickly, the research of WSN is growing more and more necessary. The most significant problem which threatens the successful deployment of sensor systems is privacy, there are many protocols providing the security of news content for the WSNs. However, due to the open feature of sensor networks, context information is still in an exposed state, which makes the network be vulnerable to traffic analysis attack and hop by hop tracing back packet attack. Thus location privacy protection programs have been proposed. In this paper, we analyze and compare the existing major schemes comprehensively, meanwhile illustrate their theoretical models, principles and the advantages and disadvantages in detail.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

With the rise of Internet of things, wireless sensor network (WSN) which is an integral part of Internet of things have a very broad application prospects.

WSNs consist of a large number of micro sensor nodes, those nodes are capable of sensing information, computing and communicating. However, due to the low cost of these nodes, the storage capacity of battery is small, the computing capability of node processors is low, and the communication of wireless communication device is limited. Overall wireless sensor networks have the following characteristics: large-scale, self-organizing, multi-hop routing, dynamic, resource-constrained and applications related. These features make the wireless sensor networks have broad application prospects in military, environment, medical treatment, smart home.

Wireless sensor networks could be used to collect sensitive information or deployed in hostile or unprotected environment, which make protecting the privacy of sensor nodes be crucial in the current WSNs, the privacy issues in WSNs are divided into two categories: content privacy and context privacy. In order to solve the problem of content privacy, for now, many encryption and authentication mechanisms[RFC4948][RFC4949]have been proposed and used, and can basically meet the corresponding requirements. But due to the open feature of WSNs, the exposure of context information can cause the user’s secret leak to the attacker, especially attacker can locate the source node or destination node (base station) through traffic analysis and hop track packet stream. The location of source node and base station are very sensitive in many WSN applications such as in precious animals detection system, the position of animals (source node) can’t be exposed to illegal hunters; in battlefield information collection system, the position of soldier (sink node) who accepts a variety of information can’t be exposed to the enemy. Because of the importance and necessity of location privacy, this paper has a research on principles, advantages and disadvantages of current main location privacy protection agreement (PhR[PhR](GROW[GROW], PRLA [PRLA]), PUSBRF[PUSBRF], LPR [LPR], LPSS[LPSS], DEFP[DEFP]).

Based on the property of object which needs to be protected, this paper divides the possible attackers into two categories: the attackers who attack source node and the attackers who attack sink node, and establishes corresponding models according to their individual features. According to the attacker models we propose appropriate protection agreements and discuss their advantages and disadvantages.

The main contributions of this paper are as follows:

(1) We divide possible attackers into two categories based on the property of object which needs to be protected for the first time, and establish the corresponding attack models;

(2) We put forward the corresponding settlement agreements in accordance with attack models on the basis of scientific ideas that discovering problems then solving them, meanwhile we conduct comprehensive analyses and comparisons on the main location privacy protection agreements systematically for the first time;

(3) We summarize the maximum intensity attacker that each privacy protection agreement can handle by analyzing and comparing, then conclude the respective applicable scenario of each agreement.

2. The Attack Models

The objects protected in WSNs are usually the source node (such as in precious animals detection system, the position of the node which has monitored animals can't be exposed to illegal hunters) and the sink node (such as in battlefield information collection system, the location of the last node which is responsible for transferring a variety of information to the soldiers can't be exposed to the enemy). According to the property of object which needs to be protected we divide possible attackers into two categories: the attackers who attack source node (source attackers) and the attackers who attack sink node (sink attackers). This article assumes that two types of attackers both have the following characteristics: ① attackers have excellent hardware, sufficient storage space and powerful computation ability; ② attackers can detect traffic only in one region, but are not capable of decrypting data packets [PRLA]; ③ attackers can only trace the nodes sending data packets but the nodes receiving data packets.

2.1. The Model of Source Attackers

The process of attacker tracing back source node's location is described as follows: the attacker starts monitoring at the sink node, when monitored a message, he can deduce that the signal is issued by node A through wireless signal positioning device, then moves immediately to node A to continue to wait, when a new message received he determines that it was issued by node B and then quickly moves to node B, repeat this process can trace to the location of the source node.

This paper divides the source attackers into two categories based on the sources attackers' tracking method: the patient source attacker and the careful source attacker.

The model of patient source attacker is described as follows: the attacker follows a simple and natural attack strategy: he starts on the position of sink node (base station) to wait until a new message is heard, and then immediately move to the node that generated the message, repeat this process until the location of the source node is traced.

The model of cautious source attacker is described as follows: because some privacy protection technology [3] could lead an attacker to strand at a location remote from the real source node, the strategy of cautious source attacker is limiting the eavesdropping time in one position, if he has not received any new messages within a specified time interval, he thinks that he was misled to current position, and then hops back to the previous position to continue listening.

2.2. The Model of Sink Attackers

Sink attackers determine which nodes are on the transmission path according to the time sequence of date packet transmission, then mobile hop by hop, and finally get to the sink node. The process of attacker tracking sink node’s position is described as follows: assuming the attacker listening for message transmitting within the range of one hop at node C, he monitors that node C sends a data packet at first, then node B transmits a data packet subsequently, the attacker moves to the node B immediately and infers that the transmission path at this time is C to B, according to this method, the attacker tracks the location of the nodes which are one hop from the base station as having captured the sink node.

Similarly sink attackers are also divided into two categories: the patient sink attacker and the cautious sink attacker. The principle of their attacker model is similar to the principle of corresponding source attacker model, not repeat them.

3. Location Privacy Protection Agreements

In order to prevent these attackers from destroying the location privacy security of wireless sensor networks, a series of security protocols are proposed, such as: phantom routing (PhR), source location privacy preservation protocol in wireless sensor networks using source-based restricted flooding (PUSBRF), location-privacy routing protocol (LPR), location privacy support scheme (LPSS), differential enforced fractal propagation (DEFP). This section will classify these main protocols and describe the principle of each protocol in detail.

In this paper, we divide the main privacy and security protocols which are mentioned above into three categories: source location privacy protection protocols, sink location privacy protection protocols and both location privacy protection protocol. Source location privacy protection protocols include: PhR, PUSBRF; sink location privacy protection protocols include: LPR, DEFP; and both location privacy protection protocol includes LPSS.

3.1. Source Location Privacy Protection Protocols

3.1.1. Phantom Routing (PhR)

Take the panda-hunter model[PhR] for example, the description of phantom routing is decribed as follows: in PhR , the transmission of each information goes through two phases:① the random walk phase , may be a pure random walk or a directional walk (based on sector or hop count between the node and the sink node[PhR]);② subsequent flooding/single-path routing phase, which will send the information to the sink. When the source node sends a message, the message is unicasted Hwalk hops randomly, then pass it to the base station based on the baseline (probability) flooding[SECH]or single-path routing[PhR]. Because of PhR, after an attacker intercepted messages i he will wait a long time before receiving the next message i+1, when he finally receives the message i+1, the instant sender of this message may lead the attacker to the position which is away from the true source node.

On the basis of phantom routing (PhR) also proposed the phantom routing with location angle (PRLA)[SECE], PRLA is consist of three phases:① the sink node floods a query message in the whole network, so that each node can creates the shortest path to the sink and divides its neighboring nodes into two direction collections according to the distance between neighboring nodes and the sink;② the source node produces a limited flooding with the range of random walk, this process makes each node can get the inclination angle of respective neighboring nodes and calculate the transmitting messages possibility of each neighboring node;③ the source node sends date packets to the sink node, each data packet will be transmitted Hw hops in a random walk way based on the inclination angle, then along the shortest route path goes to the sink node from the phantom source node.

PRLA is essentially an improvement of PhR’s random walk phase, to a degree it avoids the generation of the offset path[PUSBRF], on the basis of PhR it further improves the safety time.

Greedy random walk (GROW) is essentially an improvement of PhR’s random walk phase too, in GROW, the sensor node each time selects a neighboring node from those who did not participate in the random walk phase, in this way, random walking is always trying to cover a area where hasn’t accessed to by greedy strategy[GROW], thereby improving the ability of sensor networks against attackers.

3.1.2. Protocol Using Source-based Restricted Flooding (PUSBRF)

PUSBRF protocol is consist of four phases:① network security initialization phase;② source node h hops limited flooding phase;③ h hops directional routing phase, the direction of each hop is selected by the current node based on the minimum hop value that its neighboring apart from the source node;④ the shortest path routing phase.

The process of network initialization phase is described as follows: complete the establishment of the key, discover the neighboring nodes to achieve the information of minimum hop value that each ordinary nodes apart from the base station, and each node pre-loads the following parameters: the public key (Kpub) used for message encryption, the list of neighboring nodes (Tu), hop value h, then generate a base-station broadcast in the whole network, the base station broadcasts the initialization message BM={BRO_BASE,ID,hop_bs} in the entire network, in which BRO_BASE indicates the type of messages, ID indicates the identity of the node that sent the message, hop_bs indicates the hop count of the message which is initially 0., PRLA is consist of three phases:① the sink node floods a query message in the whole network, so that each node can creates the shortest path to the sink and divides its neighboring nodes into two direction collections according to the distance between neighboring nodes and the sink;② the source node produces a limited flooding with the range of random walk, this process makes each node can get the inclination angle of respective neighboring nodes and calculate the transmitting messages possibility of each neighboring node;③ the source node sends date packets to the sink node, each data packet will be transmitted Hw hops in a random walk way based on the inclination angle, then along the shortest route path goes to the sink node from the phantom source node.

The process of the source node h hops limited flooding phase is described as follows: it makes the source node realize the broadcast in whole network within h hops, each node which is in the rage of h hops from the source node gets the minimal distance between itself and the source, then in list Tu adds the minimal hop value that the neighboring nodes away from the source node and records the value.

The phantom source nodes generated in h hops directional routing phase are far enough away from the real source node and their location is diverse. The shortest path routing achieves transmitting packets from the phantom source node to the base station in a shortest period of time.

3.2. Sink Location Privacy Protection Protocols

3.2.1. Location-privacy Routing Protocol (LPR)

Because the goal of routing protocols is to transmit a packet along the shortest possible path to the destination, the packets' forwarding direction is always pointing to the receiver. Then the attacker will determine the wright node which the real package goes to according to the general trend of path. In order to resist this kind of problem LPR protocol has been proposed.

LPR randomizes routing path, so that the forward direction of packages does not always point to the receiver. The route consists of two phases: ① each sensor node divides his neighboring nodes into two lists: a closer list which is consist of the neighboring nodes whose distance to the destination is shorter than its own; a further list which is consist of the neighboring nodes whose distance to the destination is longer than equal to its own, the specific classification criteria refer to the literature [LPR]. ②When a sensor node forwards a date packet, he chooses a neighbor node in one of the two lists randomly as the next hop node of the package, and the selection probability from the further list as the next hop node is Pf, so the selection probability from the closer list as the next hop node is 1-Pf.

3.2.2. Differential Enforced Fractal Propagation (DEFP)

DEFP is a simple distributed algorithm based on DFP[DEFP]. The key idea of the program is to leave early packet forwarding nodes have a higher chance of false packet transmission in the next phase, at the beginning DEFP allocates one vote to every neighboring node. When a node selects one of his neighboring nodes as the next node which is false packets forwarded to, the votes of the node increase k. According to this approach, after using lottery scheduling algorithm [SECH], when a node has forwarded a fake packet to one of its neighboring nodes, it will continue to forward other fake packets to the same neighboring node with rising probability.

3.3. Both Location Privacy Protection Protocols

The program consists of two phases:① Each sensor node divides his neighboring nodes into three sets: a small gradient [SECT]set comprised of the neighboring nodes with smaller gradient value; an equivalent gradient set comprised of the neighboring nodes with the same gradient value; a large gradient comprised of the neighboring nodes with larger gradient value. ② When a neighboring node transmits a packet, he selects the next hop node from the equivalent gradient set with the probability Pi, or selects the next hop node from the small gradient set with the probability 1-Pi. LPSS also can be used combine with the fake package strategy.

4. Performance Comparison

This section compares the performance of the location privacy security protocols mainly by three parameters: security strength (safety time), transmission delay, communication overhead.

(1) Safety time (privacy protection strength): the number of packages sent by the source node before the target node exposed to the enemy (before hunters capturing the panda or enemy discovering soldiers who receive information), the more of packages be sent the longer of safety period, conversely the shorter of safety period;

(2) Energy loss (communication overhead): the average hop value through which the data packet sent by the source node eventually arrives at the sink node (base station), and the lager of the hop value the greeter of communication overhead, conversely the smaller of communication overhead;

(3) Propagation delay (transmission delay): the period in which the data packet sent by the source node eventually arrives at the sink node (base station), obviously lager of the average hop value the longer of transmission delay, conversely the shorter of transmission delay. Combining with the consequence in (2) can easily conclude that the communication overhead is proportional to transmission delay.

In order to facilitate the comparison, source location privacy protection protocols all use the same simulation configuration: in the OMNet[SECT]simulation environment, we distribute 10000 sensor nodes uniformly in the network with area of 6000*6000 m2, in which the communication radius of each node is 110m. So the average number of neighboring nodes of each node is 8.64, weakly connected nodes (node number of neighboring nodes is less than or equal to 3) account for only about 1%, the attackers begin tracking from the base station.

The communication overhead is closely related to two parameters: the hop value of random walks and the distance between the source node and the base station. When research the changing trend with one parameter, we need to assume the other parameter as a fixed value. Assume that the distance between the source node and the base station are 60 hops, the relationship between communication overhead and hop count of random directional walks shows that:① With the number of random directional hops increasing, the communication overhead (average transmission delay) of PhR and PUSBRF both increase. This is because with the number of random directional hops increasing, date packets need forward more times during random routing phase to reach phantom source nodes, however, this phase doesn’t make contribution to pass packets to the base station, thus their communication overhead improves.② When the random directed hop value is fixed, the communication overhead of PUSBRF is slightly higher, because the directed walk of PhR is based on the number of hops between the node to the base station, so PhR only need the base station broadcast in the whole network, but from the above mentioned phases of PUSBRF protocol we can see, PUSBRF requires not only the base station broadcast in the whole network but also needs the source node broadcast in the whole network within h hops.

Make the value of random directional hops as h=15, then the trend of the two protocols between the communication overhead and hops from the source node to the base station shows that: ① the communication overhead (average transmission delay) of PhR and PUSBRF both increase with the distance between the source node and the base station increasing. This is because with increasing distance between the source node and the base station, the data needs to go through more hops to reach the base station.② when the hop value of two protocols between the source node and the base station are the same, the communication overhead of them are about the same.

(3) The security period is closely related to two parameters: the value of random directional hops and the distance from the source node to the base station. Assume that the distance between the source node and the base station are 60 hops, then the trend of the security period and the random directional hop value shows that: ① The security period of PhR and PUSBRF both increase with h increasing. This is because the increasing h makes the distance between the phantom source nodes generated by two protocols and the real source node further, then generates more random paths which make the source attackers more difficult to trace. ② When the random directional hop value are the same, the security period of PUSBRF is much longer than PhR’s, this indicates that the safety performance of PUSBRF is better than PhR’s. This is because phantom source nodes generated by PUSBRF are more diverse geographically than which are generated by PhR[PRLA].

Make the value of random directional hops as h=15, the trend of the security period and the distance from the source node to the base station shows that: ① With the increasing of the hop count between the source node and the base station, the security period of PhR and PUSBRF also increases. This is because when the hop count is larger, the more hops that source attackers need to trace back to the real source node. ② When the hop count between the source node and the base station of two protocols are the same, the safety performance of PUSBRF is better than PhR’s, indicating that the safety performance of PUSBRF better than PhR, the reason is the same as above.

The performance comparison of above two protocols and LPSS used with fake packets shows that: the safety performance of pure LPSS is between PhR and PUSBRF, so are communication overhead and transmission delay, when LPSS is used with the false packet strategy, the safety time increased substantially and the communication overhead becomes larger, but the transmission delay is still close to pure LPSS protocol, which is because the transmission paths of true packets are the same with pure LPSS, fake packets just used to confuse attackers, and don’t affect the transmission of true packets.

In summary, compared to the pure flooding and single- path routing, PhR can resist the attacker’s packet tracing attack to some extent, but the phantom source nodes generated by PhR concentrate in one area with high probability; PUSBRF protocol makes up this deficiency, it can generate phantom source nodes which are geographical diversity with equal probability, and enhance the security of the source node’s location privacy effectively, however the improvement of security period at the cost of increasing of communication overhead, so the communication overhead of PUSBRF is more than PhR’s, the transmission delay is longer too, and can’t weigh between the security period and the communication overhead; gets the weigh between security period and transmission delay by adjusting the value of the parameters Pi. When LPSS is used combines with false packet strategy, it can achieve impressive safety performance, but at the cost of communication overhead increasing.

The above three protocols can withstand source attackers (including patient source attackers and cautious source attackers), and are more resistant to cautious source attackers[SECW], their pros and cons make we should select the appropriate protocol according to specific application requirements.

The simulation results of location privacy protocols which can protect the sink node (base station) are shown as follows:

In order to facilitate the comparison, sink location privacy protection protocols all use the same simulation configuration: in the OMNet simulation environment, we distribute 2500 sensor nodes uniformly in a sensor network, make the average number of neighboring nodes of each node be 8, and attackers began tracking from the source node.

(1) At the packet forwarding phase LPR protocol selects the next hop node from the further list with probability Pf, and get the trend between the transmission delay and hop count from the source node to the sink node of pure LPR when Pf is 0.0%, 25%, 37.5%, meanwhile compare with DEFP. The resulet showa that: ① with the increasing of distance between the source node and the base station,

the transmission delay of two protocols both increase. This is because when the source node is far away from the base station, sink attackers at the source node need to track more hops to reach the base station;② when the distance from the source node to the base station are the same in LPR, the transmission delay increases with the increasing of Pf. This is because Pf is the probability with which we select the next hop from the further list, the larger of Pf the more likely to choose the next hop from the further list, which extends the transmission path;③ when the distance between the source node and the base station are the same, the transmission delay of LPR is longer than DEFP’s.

(2) The trend between security period and Pf of pure LPR protocol and compare with DEFP shows that: ① with the increasing of Pf, the security period of LPR increases. This is because Pf is the probability with which we select the next hop from the further list, the larger of Pf the more likely to choose the next hop from the further list, which extends the transmission path, so sink attackers need trace a longer time to reach the base station;② the security period of LPR is longer than DEFP’s, and the larger of Pf, the higher amplitude of LPR’s security period longer than DEFP’s.

The performance comparison of above two protocols with fake packets strategy, pure LPSS and LPSS with fake packets strategy indicates that: when DEFP, LPR, LPSS all used with fake packets strategy, the security period of three protocols all improving, the transmission delay remain constant, but the energy consumption increasing.

In summary, LPR can get the balance between privacy protection strength (security period) and energy consumption by adjusting Pf, LPR with fake packets strategy can effectively improve the safety performance of the program compared with DEFP, but its transmission delay and communication overhead are far greater than DEFP’s, LPSS get the trade-off between transmission delay and security period by adjusting Pi, and with the increasing of hop counts between the source node and the sink node, the safety strength (security period)of LPSS increases evidently dramatically than LPR, but LPSS can only play full advantage when it is used with fake packets strategy, otherwise it isn’t superior than LPR and DEFP comprehensively.

The above three protocols can resist sink attackers (including of patience sink attackers and cautious sink attackers), and they all have their pros and cons, we need select the appropriate protocol according to specific application requirements.

5. Security Consideration

This paper divides attackers into two types based on the properties of the objects which need be protected: source attackers and sink attackers, then establishes corresponding attack models, after that we propose appropriate protocol in accordance with attack models, including phantom routing (PhR), source location privacy preservation protocol in wireless sensor networks using source-based restricted flooding (PUSBRF), location-privacy routing protocol (LPR), location privacy support scheme (LPSS), differential enforced fractal propagation (DEFP). At last we have comprehensive analysis and comparison of these location privacy protection protocols systematically, mean while sum up the advantages and disadvantages of each protocol.

6. IANA Consideration

To be completed.

7. References

[RFC4948] Perring, A., Szewczyk, R., Tygar, D., Wen, V., and D. Culle, "Spins: security protocols for sensor networks", May 2007.

[RFC4949] Eschenaur, L. and V. Gligor, "A key-management scheme for distributed sensor networks", August 2007.

[PhR] Kamat, P., Zhang, Y., Trappe, W., and C. Ozturk, "Enhancing source location privacy in sensor network routing", August 2005.

[GROW] Xi, Y., Shi, W., and L. Andersson, "Preserving source location privacy in monitoring-based wireless sensor networks", August 2006.

[PRLA] W P, Wang., Chen, L., and Wang. J X, "A source--location privacy protocol in WSN based on locational angle", August 2008.

[PUSBRF] Juan, C., Binxing, F., and Y. Lihua, "A Source--Location Privacy Preservation Protocol in Wireless Sensor Networks Using Source--Based Restricted Flooding", August 2010.

[LPR] Jian, Y. and S. Chen, "Protecting Receiver-Location privacy in Wireless Sensor networks", August 2007.

[LPSS] Kang, L., "Protecting location privacy in large--scale wireless sensor networks", August 2009.

[DEFP] Deng, J., Han, R., and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks", October 2005.

[SECH] Cheng, Z. and W. Heinzelman, "Flooding Strategy for Target Discovery in Wireless Networks", April 2003.

[SECE] Waldspurger, C. and W. Weihl, "Lottery scheduling: Flexible proportional-share resource management", November 1994.

[SECW] Ouyang, Y., Le, Z., Chen, G., Ford, J., and F. Makedon, "Entrapping adversaries for source protection in sensor networks", Jone 2006.

[SECT] Mallanda, C., "Simulating Wireless Sensor Networks with OMNeT++[EB/OL]", Jone 2000.

Authors' Addresses

Lin Zhou
SouthEast University
SouthEast University,Nanjing,210012

Email: 573823136@qq.com

Jie Huang
SouthEast University
SouthEast University,Nanjing,210012

Email: jhuang@seu.edu.cn