International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Bidirectional Location Privacy Protection Schemes against Internal Adversary in WSN

Samson Raja T[1], S. Satheesbabu [2], Dr.K.Balasubadra[3]

[1]PG Scholor, PSNA College of Engineering & Technology, Dindigul, Tamilnadu-624622, India

[2]Associate Professor, PSNA College of Engineering & Technolgy, Dindigul, Tamilnadu-624622, India

[3]Professor, RMD Engineering College, Kavaraipettai, Tamilnadu-601 206, India

Abstract: ***Wireless sensor networks (WSNs) consist of numerous small nodes that collect and spread the information for many different types of applications. The major use of WSN is tracking and monitoring the objects, such that the observed objects are also needed the protection. For instance, a WSN can often deploy in hostile environments to detect and collect interested events such as the appearance of a rare animal. However, due to the open characteristic of wireless communications, an adversary can detect the location of a source or sink in networks. Thus the location privacy of both the source and sink becomes a censorious problem in WSNs. Previous research only focuses on the location privacy of the source or sinks independently. A new research proposes the implementation of four location privacy schema to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper. But, the introduced four location privacy schemes have different performance on protecting the single stationary source, sink or both. As the proposed work, we plan to decompose the provided schemes and analyze the safety period, end to end latency, energy consumption by introduce the new scheme "The tree diversionary protection" for location privacy at source and sink respectively. Also focusing on optimal combination can be discovered to achieve a highest end to end location privacy protection for multiple mobile sources. Simulation results show that our scheme is very effective to improve the privacy protection while maximizing the network lifetime.***

Keywords: **Local Adversary, tree diversionary, location privacy wireless sensor networks**

1. Introduction

Recent advancement in wireless communications and Micro-Electro-Mechanical Systems (MEMS) has enabled the development of low-cost Wireless Sensor Networks (WSNs), which are made up of a number of sensor nodes that are self-organized for various applications, such as mobile target detection. Due to the open characteristic of wireless communications, it is not difficult to attack wireless sensor networks with the goal of either obtaining confidential data or simply disrupting the normal operations of the WSN applications.

In Wireless Sensor Networks (WSNs) are formed by battery-powered devices commonly used for environmental monitoring, military surveillance, and industrial automation etc, The recent researches focus in sensor are low-power with high exchanging of information, and battery lifetime are well organized with the financially expenses of such devices are paving the way for a widespread use of WSNs in a vast array of the application

In Previous research focuses on proposed four location privacy schemes of both the source and sink, the four schemes namely, Lukewarm potato model, Duplex privacy scheme, Secure location protection using fake nodes, Base station location anonymity and security technique. but since the four schemes has different performance on protecting the source location privacy or sink location privacy.

As the proposed work, we plan to decompose the provided schemes and analyze the safety period, end to end latency, energy consumption by introduce the new scheme "The tree diversionary protection" for location privacy at source and sink respectively. Also focusing on optimal combination can be discovered to achieve a highest end to end location privacy protection for multiple mobile sources. Simulation results show that our scheme is very effective to improve the privacy protection while maximizing the network lifetime**.**

The main theme of this paper can be follows:

1. We address the importance of simultaneously protecting the location privacy of both the source and sink.
2. For that we analysis and compare the previous four schemes for end to end location privacy
3. But since the four schemes has different performance on protecting the source location privacy or sink location privacy
4. In this paper we introduce the new concept for location privacy by using the tree diversionary protection scheme.

1.1 Metrics of End to End Location Privacy Protection

We use the following three metrics, safety period, latency, and energy consumption to evaluate the proposed end-to-end location privacy protection schemes:

- ***Safety period:*** The safety period started from the moment the adversary, pointing the tracing rules and ends at the moment when the adversary find out the source or sink.
- ***End-to-end latency*****:** The end-to-end latency is defined how much time taken for a packet travel from source to sink. That is its measure the average time taken from source to sink
- ***Energy consumption***: in this project we only consider packet transmission requires an equal amount of energy and the energy consumption is measured in terms of the average number of packets transmitted in the network within period.

2. Related Works

The location privacy protection most growing and hot researching topic in wireless sensor network. Most of the existing schemes are mention only the source side of the location privacy or sink side of the location privacy independently. The major disadvantage is none of them consider the location privacy of both source and sink simultaneously. Such that in recent years, the research are focuses on the field of end to end location privacy against local adversary in WSNs.

In that the most popular end to end location privacy schemes are (1) Lukewarm potato model, (2). Duplex privacy scheme, (3) Secure location protection using fake nodes, (4) Base station location anonymity and security technique.

Such that four recent end to end location privacy protection schemes are focusing the safety period, to measure the safety period is started from the moment of adversary until the adversary will find out the original node of the data in source side. The second stage is monitoring the end to end latency between the average time take from source to sink and the final stage is defined the energy consumption it shows the communication between the source to sink in equal amount of energy.

The first model of the end to end location privacy scheme **lukewarm potato model** which is defines as, randomly choosing the nearby node to deviate the adversary. If the monitoring packets are delivery form source to sink in same and fixed path means than the eavesdropper can easily hack and identify the location of the entire path of the source and sink via node by node counting.

To avoid this problem the lukewarm potato model is used to achieve the end to end location privacy protection by choosing the randomizing the delivery path. In LPM have a three major list to choosing the nearby node that is closer list, equivalent list and further list.

The list that contains the hop count Hi and node Ni. In that the closer lists handle the each node in Ni with a smaller than hop count Hi denoted in closer list. The equivalent list is defines the each node in Ni with the equal count to the Hi and each node in Ni with a hop count larger than Hi will be included into further list.

In lukewarm potato list contains the union of closer list and equivalent list. The initialization step is to check next_hop =null. If the hop count is null than lukewarm potato list was created. While receive the message than randomly choose a nearby node from LPL to the next hop and forward the received packet to the next hop. Since this model is increase the end to end latency and safety period is dose not high.

The second end to end location privacy model is **Duplex privacy scheme** which is defines as, creating the dummy message and backtrack to original message for Deviate the adversary. Such that, real messages travel along the shortest route from the source to the sink node and branches are designed along the shortest route. Then the Source side travel dummy messages from leaf nodes which make to deviate adversary. The each branch are generating Dummy message to back track the original message travel from source to destination. Those all the process is done when local adversary involved during the time of data transmission from source to destination.

If suppose the destination node got the dummy message means it destroy the whole delivery path and again choose the new nearest path from source to destination for data transformation. In that each original data node having the same fixed packet size. Based on that the destination node can easily find out the original node and dummy node. Here the problem and major disadvantage is smart hacker can easily hack and find out the original data node during the communication between source to sink and also the tree branch are created in both source and sink side for that the time latency is very high and energy capacity is very low.

The third model of end to end location privacy protection is **secure location protection using fake nodes**. In this scheme we can create and deploy the dummy nodes for both source and sink tree branch. The dummy nodes only pass the dummy message from source to destination based on the dummy node we can able to easily deviate adversary by integrated to the original node.

If any adversary is backtrack to the original data than the dummy node from child branches will be integrated to the original node and pass through the destination path. The path of the data transformation must be selected in random once or dynamic once.

If the sink node got the dummy message than it will reselect a child node to relay this dummy message. And this model we are deployed own dummy nodes such that the life time of the nodes energy is very poor and also the end to end latency is high.

The fourth and another end to end location privacy protection scheme is **Base station location anonymity and security technique.** In this model we create the proxy source and proxy sink to make the real messages be delivered random path. Here the process is from the source to the proxy source, from the proxy source to the proxy sink and from the proxy sink to the sink.
The source only chooses the proxy source based upon the shortest path and the proxy source cannot be choosing the nearby sink of the proxy sink. If the proxy source or proxy sink capture the adversary then the whole delivery path will be blocked and it choose another nearby pat for sending the data from source to destination.

Here also we can create the dummy nodes in both sides of tree branches for passing the dummy message to deviate the adversary. The main drawback for this model is implementation of proxy in source and sinks side. If we want to provide high location privacy in large area then it is very difficult.

3. Proposed Method

In this paper, we propose a novel tree diversionary protection scheme for protecting location privacy based on

hiding and seeking the strategy to create diversionary or decoy routes along the path to the sink from the original source at the end of the each diversity path to be discarded, which periodically release the dummy message. We also focusing to maximum the network lifetime and reduces the energy consumption with the high safety period. As well as we can create the redundant diversity path in non hotspot regions with abundant energy. The proposed scheme must be satisfied the following method: (1) the routing trees established are homogeneous and adversary cannot infer the source location based on the shape of the tree and the historical trajectory of the routing path. (2) The node must be contain energy consumption in hotspots that is not increased and the network lifetime is not decreased (3) The abundant energy in the region away from the sink is utilized to build redundancy diversionary routes, so that it is difficult for the adversary to trace to original data node.

The implementation of TDP is divided into two design method: (1) establish the backbone route path direct to the network edge based on the existing original data routes, and improve the historical trajectory in order to avoid direction-oriented attacks by implementing homogeneous trees. (2)Establish redundancy diversionary routes as many as possible in regions with abundant energy to satisfied the energy consumption and network lifetime

The main idea is that we establish the original node away from the source node and then establish tree branch path towards the sink with strategically created diversionary routes as its branches, and also we can create the diversionary routes. The ends of these diversionary routes are dummy source nodes to be decoy.

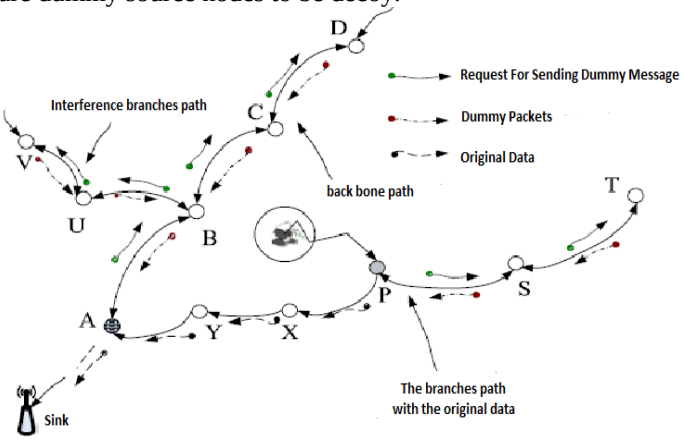

Fig 1 .Establish the process of TDP

Previous research has shown that, attacker can still trace to the source node with a relatively high possibility. Therefore, one possible solution is to make it difficult for attacker to trace to the original node, so that will be impossible to trace the source node. The TDP first establishes a backbone path direct to the network border with diversionary routes as its branches. Then, it establishes diversionary routes as many as possible with each diversionary route directing to the network border, forming a tree based routing path. The data packet length and the data generating possibility are the same in each diversionary route

4. Algorithm for TDP

Tree-Based Diversionary protection:

Based upon the network model the tree based diversionary protection schemes include three important stages that is (1) Tree-based diversionary routing establishment; (2) Stable operation stage of the tree-based routing path, (3) Destruction of tree-based diversionary routing.

Establish Tree-based diversionary route with original node. First, establish the branch with original node, and then establish the tree trunk and other branches. Generally, original node cannot be the node on the backbone routing path, because the backbone route is relatively easy to identify, and therefore the original node is more vulnerable to be find out. If the original node is not on the backbone path, it can be on any existing branches; therefore it is diff□cult for adversaries to trace. The establishing process of branch with original node is as the following two directions.

In left-down direction the original node P selects node X from its neighbor nodes, which is the node closest to the sink and on the left of P according to the left-hand rule. Then, X selects node Y which is on the most right of X and with the same hops as X to the sink according to the left-hand rule, then selects the most left node closest to the sink, i. e., alternately selects the node closest to the sink and the node with same hops, until the transmission distance reaches the hops ø namely, node A we call it the intermediate node.

The upper right direction of original node P. P sends request packet containing information of ``request sending dummy packets" to the most right node S, and the sending frequency of dummy packets is included in the request packet, which indicates node S should send dummy data packets to P in the fixed time. Similarly node S sends request packet to node T, then T get the request and sends dummy packets to S, and so on, until reaching the network border, then the branch route with original node is established.

Creating Tree

1: create original node P use the same algorithm as reference [6]
2: σ =random(0,1)
3: If $\sigma \geq \frac{1}{2}+\frac{1}{h}$ then ϑ ="right" Else ϑ ="left"
4:P(claim) ← <ID_p,type, Φ ,branch_loactions, τ , ϑ , padding_data>
5:p(sign_claim) ← k_p^x (<ID_p,type, Φ , branch_loactions, τ , ϑ , padding_data>)
6: next_node=*P*
6.1:while (next_node(sign_claim). Φ >0)
Alternately select the next_node as the next hop based on the following two strategies
next_node = GetNextOnLeastHop(current_location, ϑ);
next_node = GetNextOnEqualPath(current_location, ϑ);
$\Phi = \Phi$ -1
End
6.2: A= next_node
6.3: next_node=*P*
6.4: while (next_node has not reached network border)
Alternately select the following next_node as the next hop
next_node = GetNextOnMaxHop(current_location, ϑ);
next_node = GetNextOnEqualPath(current_location, ϑ);
End
7: for node A respectively runs 7.1 and 7.2
7.1: while (GetNodeOnMinHop(A) is not sink)
A= GetNextOnMinHop(A)
End
7.2 while (GetNextOnMaxHop(A) not reach network border)
A= GetNextOnMaxHop(A)
End
End
8:for each node *B* in the backboneroute
If B.hop is in branch_loactions
next_node=*B*
while (next_node have not reach network border)
Alternately select the following next_node as the next hop
next_node = GetNextOnMaxHop(current_location, ϑ);
next_node = GetNextOnEqualPath(current_location, ϑ);
End while
End if
End for

Creating Branches Routing

9: for each node C on the tree route
when the fixed time τ comes, do the following
if *C* receives the real data packet
Send the real data packet to GetNextOnMinHop(C);
else
Send dummy packets to GetNextOnMinHop(C);
End if
End for

Eliminate Branches connection if the adversary is available

10: If a node receives a "stop" packets
Send packets to all neighbors in the tree route
Stop transmitting any packets
End if

Stable Operation Stage of TDP:

In the Stable Operation Stage of TDP, If the original data packet is received, then the node sends the real data packet when it comes to the transmission time, if not, dummy message is generated in a specific time and sent when it comes to the transmission time.

Destruction of Tree-Based Diversionary:

The destruction of tree route is relatively simple, which depends on the original node P, and intermediate node A. if node P and node A have not received the original data packets within the time out interval, this routing path will be discarded. Node P and node A will send message to nodes involved in the route to discard once all the path get the stop information, they will no longer send any message. Thus, the entire route stops sending message.

Establish the backbone path from sink to source:

In this part, we will discuss the location of the backbone path from sink to source to achieve security. With original path of strategy there is only one original path, which is the shortest path from phantom node to the sink, so the route path depends on the original node.

We identify a novel attack method called direction-oriented attack, which has good attack performance and can effectively attack the privacy preserving strategies based on original node routing path, and it shows that there is still potential security hazard by randomly selecting original node. Therefore, in this work, we propose a new strategy to avoid direction-oriented attack in tree based diversionary routing.

5. Conclusion

The end to end location privacy is most important issues in WSN. In this paper we discuss about previous four end to end location privacy schemes and its drawback regards safety period, energy computation and latency. To overcome this problem we proposed one new scheme is called Tree Diversionary protection schemes. In that scheme we achieve and overcome the previous problem. As well as we can consider about the direction based attack to avoid and deviate the internal adversary. Finally we discuss in this capture about the backbone routing path, original node travelling path, dummy nodes placed in the TDP for providing the location privacy to achieve safety, energy and latency.

References

[1] P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, Enhancing source-location privacy in sensor network routing, in: Proc. of IEEE ICDCS, 2005, pp. 599–608.
[2] P. Medagliani, J. Leguay, G. Ferrari, V. Gay, M. Lopez-Ramos, Energy-efficient mobile target detection in wireless sensor networks with random node deployment and partial coverage, Pervasive Mob. Comput. 8 (3) (2012) 429–447.
[3] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, J. Anderson, Wireless sensor networks for habitat monitoring, in: Proc. of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, SPINS: security protocols for sensor networks, Wirel. Netw. 8 (5) (2002) 521–534.

[5] H. Chen, W. Lou, Z. Wang, A consistency-based secure localization scheme against wormhole attacks in WSNs, in: Proc. of IEEE International Conference on Wireless Algorithms, Systems and Applications, WASA, 2009.
[6] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, G. Cao, towards event source unobservability with minimum network traffic in sensor networks, in: Proc. Of the First ACM Conference on Wireless Network Security, WiSec, 2008, pp. 77–88.
[7] Y. Li, J. Ren, Preserving source-location privacy in wireless sensor networks, in: Proc. of IEEE SECON, 2009.
[8] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, ``Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1501_1514, 2009.
[9] H. Chen and W. Lou. (2014). On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. *Pervas.Mobile Comput.* [Online]. Available:http://dx.doi.org/10.1016/j.pmcj.2014.01.006
[10] A. Jhumka, M. Bradbury, and M. Leeke. (2014). Fake source-based source location privacy in wireless sensor networks. *Concurrency Comput., Pract. Experience* [Online]. Available: http://onlinelibrary. wiley.com/doi/10.1002/cpe.3242/pdf

Author Profile

Samson Raja T, received his M.Sc (Software Engineering 5Year) Degree from M.Kumarasamy College of Engineering, Karur Under Anna University Tamilnadu in 2012 and pursuing M.E. in Computer Science & Engineering from PSNA College of Engineering Tamilnadu under Anna University Chennai. His current Research areas include Wireless sensor networks, location privacy.

Mr. S. Sathees Babu, received his B.Sc. Degree in Physics in 1996 through Vivekananda College, Sholoavandan, Madurai Kamaraj University and M.C.A. Degree in 1999 through the R.V.S. College of Engineering and Technology, Dindigul under Madurai Kamaraj University. He did his M.E. Degree in Computer Science and Engineering in 2006 under Anna University. He is pursuing his Doctorate Degree in Information and Communication Engineering from Anna University, Chennai. He has 16 years of teaching experience to UG and PG classes and has guided many B.E. and M.E projects. His research interests are Wireless Networks, Middleware Technologies and Distributed Computing. He has published 4 papers in International Journals and 15 papers in conferences in National and International levels. He is a Life member of Indian Society for Technical Education.

Dr. K. Balasubadra, received her B.E. Degree in Electronics and Communication Engineering in 1988 through PSNA College of Engineering and Technology, Dindigul Madurai Kamaraj University and M.E Degree in Applied Electronics through the Government College of Technology, Coimbatore under Bharathiar University in 1997. She did her Doctorate Degree in Information and Communication Engineering from Anna University, Chennai, in 2009. She has 24 years of teaching experience to UG and PG classes and has guided many B.E. and M.E projects. Presently she is guiding ten PhD scholars and she is a research paper reviewer in conferences in National and International levels. Her research interests are Analog VLSI, Optical Communication and Wireless networks. She has published 5 papers in International Journals and 15 papers in conferences in National and International levels. She is a Life member of Indian Society for Technical Education and was a member in IEEE for more than 10 years. She is a recognized research supervisor of Anna University of Technology, Madurai.