Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secured Approaches to Sink Location Privacy Protection in Wireless Sensor Network

Abhishek R. Malviya, Balaso N. Jagdale

Department of Information Technology
MIT College of Engineering, Pune,
Maharashtra, India

Abstract*—Wireless Sensor Network (WSN) is a broad network consisting of a number of sensor nodes in it. WSN is used mainly for monitoring and data aggregation purpose. A best plan of opponent may to attack the sink node which is the aggregation point for the whole network. So, first there comes a need to secure the sink node from adversary. There are previous work are done by providing location privacy to sink node that are capable of defeating the limited adversary called local eavesdropper who can only observe network traffic in a small region but very few techniques has been proposed to achieve protection against the stronger adversary called global eavesdropper. This paper formalizes the essence of various sink location privacy-preserving schemes for wireless sensor networks and the proposed approaches first tries to modify the existing sink location privacy protection scheme by creating zones in the network and other keeps the sink mobile in the network and both tries to increase privacy protection strength of the network.

Keywords*—Context oriented security;eavesdropper;location privacy; sink node; wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks (WSNs) are composed of a large number of sensor nodes that are self-organized to carry tasks in military and civilian applications such as battlefield surveillance, forest fire detection, patient health monitoring, and smart environment. In a WSN, sensor nodes are densely deployed so that neighbor nodes may very close to each other. Hence, multi-hop communication in a WSN is most commonly used than a single-hop communication in order to consume less energy. Each node collects data from its environment and transports data to the receiver via a multi-hop network, performing the routing function. The open nature of WSNs makes it normally operate in unattended or hostile environments, which is easily exposed to a variety of attacks such as eavesdropping, node compromising and physical breach. The worst thing is that an attacker may try to attack the sink node itself which is the aggregation point for the complete network data. This kind of attack can make the sink a single point of failure for the whole network.

Privacy in WSNs may be classified into data-oriented privacy and context-oriented privacy in fig.1. Even after strong encryption and authentication mechanisms are applied to protect data privacy, it can be classified into data

aggregation and data query. Data aggregation is to be done by calculating mean, standard deviation, variance etc. the context information such as the location information of the source or the receiver can be deduced by eavesdropping the network traffic and analyzing the traffic patterns. Context-oriented privacy protections can be classified into location privacy preserving techniques and temporal privacy preserving techniques. Location privacy includes data source location protections and receiver location protections. Location privacy is extremely important in WSNs. In this paper, we focus on the receiver location privacy in WSN.

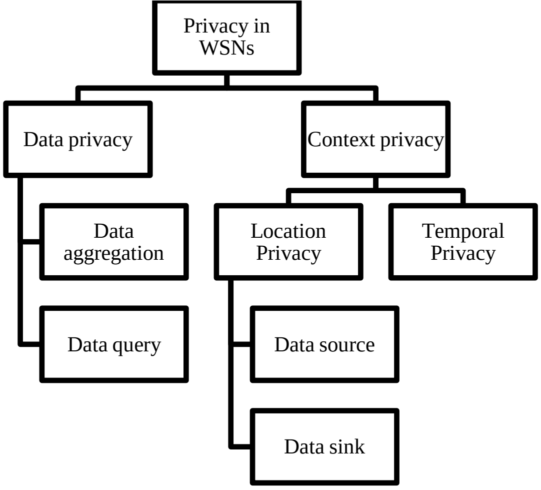

Fig. 1. Classification of privacy in WSN[1].

Generally, there are two ways for an adversary to locate the receiver: traffic analysis and packet tracing Compared with packet-tracing, traffic analysis was firstly used by attackers. An attacker can determine the receiver location by analyzing the network traffic because sensors near the receiver forward a greater volume of packets than sensors further away from the receiver. Later, packet tracing is used to find the source location because adversaries may use radio frequency localization techniques to perform hop-by-hop trace. During packet tracing, an adversary must move quickly because he does not have to stay longer at each location in order to compute the traffic density. In this paper, we focus on studying the defense measures against the traffic analysis attack.

II. LITERATURE SURVEY

This section gives a brief discussion of some sink node location privacy techniques in WSN. In [1] author has discussed the Sink Location Privacy Protection Scheme in which the basic idea is to increase the path diversity and improve the difficulty of being traced. In this scheme, real packets are sent to the real sink and face packets are sent to the fake sinks and some other random destinations. Because real packets are confused with fake packets, an adversary will spend more time in tracing the wrong directions. In this scheme, the nodes responsible for the fake packet injection are the intersection nodes of several shortest paths.

The author proposes the basic routing protocol for sink location privacy called as Location Privacy Routing(LPR) protocol in [2, 3]. This scheme is used along with the fake packet injection which uses randomized routing to confuse the packet tracer along with fake packets that make the transmission completely random. But, this technique involves increasing amount of overhead and it is not energy efficient as well. Careful monitoring of packet sending time may allow an adversary to get information about the data traffic flows. Setting the packet sending rate control between a parent node and its children nodes is the solution to this.

In Sink Simulation approach explored in [4, 5, 6] fake sinks are established in the network. The fake sinks are simulated within the communication range of real sink. When an event is detected, the source node must transmit the packet to the fake sinks in the network. So the entire fake sinks will receive the report about the event. The fake sinks broadcast the packet locally to the real sink. So it's must that the real sink should be in the communication range of at least one of the fake sink. In backbone flooding [2, 3, 4] backbone is created with a set of sensor nodes. Whenever an event is detected, the data is transmitted to the backbone member. This backbone floods the packet to the entire network. The packets about the event detected are sent to the backbone alone and real sink can receive from the backbone member. So the real sink must be in the communication range of at least one of the backbone member. In [7, 8] author proposes a Base station Location Anonymity and Security Technique(BLAST) that aims to secure the base station from both packet-tracing and traffic analysis attacks and provides good privacy against the global attacker. Network is divided into blast nodes and ordinary nodes. Receiver is present somewhere nearby blast nodes. Source node sends the packet to one of the blast nodes which is then retransmitted inside blast region. The adversary is unaware of the communication between blast node and the actual receiver. Hence, location privacy of the receiver is maintained. The next technique that the author proposes in [8] is to divide the whole sensor network into small groups called clusters using some efficient clustering algorithm. This scheme proposes some improvement of the blast technique in order to improve its performance. A cluster contains many members and a cluster head. An efficient shortest path algorithm is used to send data from the source node to the blast node. Finally, the packet reaches the nearest blast node via the shortest path. Now, packet is retransmitted within the blast security ring using varying transmission power depending upon location of the sink node. But, packet is received by the actual sink node only and the opponent is unaware of this actual receiver of data as the packet was transmitted around the whole ring. Thus, it is very difficult for him to trace the exact location of sink node even after many trials.

In [9] random data collection scheme is designed to provide location privacy to mobile sinks. It comprises two steps, the random data forwarding storage and random Movement of sink in data collection. Whenever the sensor has data to forward it encrypts the message with symmetric key and forwards along the random path storing a copy locally. The location or ID of the destination is not included in the message so that attackers fail to obtain the destination of the message. When node forwards the message it selects any node randomly as the next hop and increments the hop count by one. Then, mobile sink moves around the network to gather data from the sensors and store it in its buffer. To evade from getting attacked and tracked, mobile sink changes its moving direction randomly. Another scheme for location privacy is Randomized Routing with Hidden Address (RRHA) [10]. As the name suggests, the identity and location of the sink is kept private in the network to avoid it to be revealed and to become the target of attack. The destination addresses of the packets are kept hidden so that the attacker cannot obtain the location of the sink even when he reads the header fields of the packets. The packets are forwarded along different random paths. RRHA provides strong protection for the sink privacy against both active and passive attackers.

III. REVIEW AND ANALYSIS

Table I Comparision of sink location privacy techniques

	Privacy	**Overhead**	**Delay**	**Power Consumption**
Sink Location Privacy Protection Scheme	Excellent privacy against local adversaries	Overhead is high	No extra delay	Extra power is consumed
Sink Simulation	Excellent privacy	No extra	Very	Very less extra

	against global adversaries	Overhead	less extra delay	power is consumed
Backbone Flooding	Excellent privacy against global adversaries	No extra Overhead	Very less extra delay	Extra power is consumed
Location Privacy Routing	Excellent privacy against local adversaries	Overhead is high	Very less extra delay	Extra power is consumed
Blast Scheme	Good privacy against the global attacker	No extra Overhead	Very less extra delay	Extra power is consumed
Enhanced Blast Scheme	Excellent privacy for sink node	Overhead is high	Very less extra delay	Very less extra power consumption
Random Data Collection Scheme	Excellent privacy for sink node	Overhead is high	Delay increase	Very large extra power is consumed
RRHA Scheme	Excellent privacy for sink node	Very less overhead	Very less extra delay	Very less extra power consumption

IV. PROPOSED SCHEME

Many techniques have been proposed for the location privacy of the sink node in the wireless network. This paper proposes two new approaches to sink location privacy protection in wireless sensor network which are as follows.

A. Zone Based Sink Location Privacy

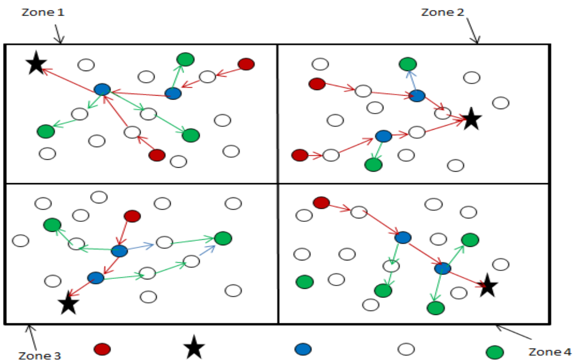

Fig. 2. Scenario of zone based sink locationprivacy approach

Assume the scenario of a network as described in fig.2. Consider the network with randomly deployed sensor nodes. The network is partitioned into the number of zones in which the source node belongs to the particular zone send real packet to the sink deployed in that zone.

Main objective of using zone routing protocol is:

- Extension of network lifetime.
- Reduced energy consumption.
- Use of data aggregation to reduce number of messages.
- To resist the traffic analysis attack.

The red nodes represent the source nodes. The green ones represent the fake sinks and some random destinations.The only black node represents the sink node. The blue nodes represent the intersection nodes. The real messages travel along the shortest paths from the source to the sink. Branches are designed along the shortest paths, in which the dummy messages travel from the intersection nodes to the fake sinks. Blue nodes are the nodes responsible for the fake packet injection. Not only, these nodes must possess higher energy, but also it is easy for more sophisticated attackers to find these special nodes by observing traffic. In sink location privacy protection scheme, the nodes responsible for the fake packet injection are the intersection nodes of several shortest paths which change dynamically to improve the network lifetime. The fake packets are the packets with no useful contents and used to draw an adversary away from the actual paths. Real packets are sent to the real sink and fake packets are sent to the fake sinks and some other random destinations. Because real packets are confused with fake packets, an adversary will spend more time in tracing the wrong directions. Thus, the safe time increases which make the sink location safe and private for more time (Safe time is a time spend to trace the exact location of sink node).

It is expected that the zone based sink location privacy approach will found more efficient than the existing location privacy techniques. The expected results of the proposed scheme are:

- Strong privacy protection of location of sink node from traffic analysis attack.
- Reduced energy consumption as zone is created.
- Minimized packet delay as real packets are transferred directly to the sink node since shortest path algorithm is used.
- Maximized safe time due to multiple fake paths.

B. Mobile Sink Approach

In mobile sink approach, the sink is kept mobile in the network and when source wants to send the packet to the receiver it simply broadcast the packet in the network. So, as the packet is broadcasted and sink is randomly moves in the network, it is difficult for an attacker to trace the location of the attacker even after packet-tracing and traffic analysis attack.

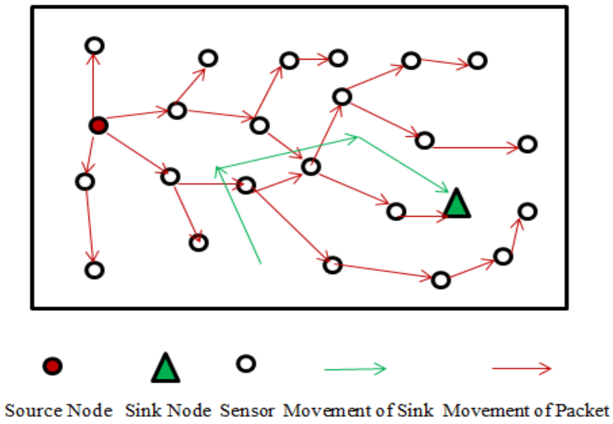

Fig. 3. Scenario of mobile sink approach

Assume the scenario of the network as described in fig.3.The red nodes represent the source nodes. The green node represents the sink node. The green arrows represent the random movement of a mobile sink in the network. Whenever a source wants to send the packet to the sink it simply broadcast the packet in the network. The sink randomly moves and collects the packet. As the sink is mobile and the packet is broadcasted it is very difficult for an attacker to trace the location of the sink node. It is expected that this approach will provide strong sink location privacy protection and we will analyze this approach in term of communication cost, delay and latency.

V.   CONCLUSION

The various sink location privacy preserving techniques are thus studied. The protocols must be strong enough to provide sink location privacy protection against any kind of attacker. Certain protocols do not work well against well-equipped adversary. Privacy protection against local or global eavesdropper can be achieved for sink nodes using fake packet injection scheme, sink simulation, backbone flooding, location privacy routing, and enhanced blast scheme respectively. These techniques provide benefits in various metrics like privacy, communication cost, and latency.

The proposed approaches provides privacy to the sink node very efficiently with the focus is on reduced energy usage, minimized the packet travel delay and to resist the traffic analysis better.

REFERENCES

[1] Lin Yao ,Lin Kang , Pengfei Shang , Guowei Wu, “Protecting the sink location privacy in wireless sensor networks,” Springer-Verlag London Limited 2012.

[2] Ying Jian Shigang Chen Zhan Zhang Liang Zhang "Protecting Receiver-Location Privacy in Wireless Sensor Networks," IEEE INFOCOM 2007 proceedings.

[3] G.Aruna Rekha, CH.TG Ramya,“Efficient and Effective Techniques for Source and Sink Location Privacy in WSN,” International Journal of Research in Computer and Communication Technology, Vol 2, October-2013.

[4] Kiran Mehta, Donggang Liu and Matthew Wright,” Protecting Location Privacy in Sensor Networks against a Global Eavesdropper,”IEEE Transaction on Mobile Computing, Vol. 11, NO. 2, February 2012.

[5] Pavitha N ,S. N. Shelke“Techniques for Protecting Location Privacy of Source and Sink Node Against Global Adversaries in Sensor,” International Journal of Research (IJR) Vol-1,September 2014.

[6] Chinnu George, Dhinakaran Nathaniel,“Protecting Location Privacy in Wireless   Sensor Networks against a Local Eavesdropper–A   Survey,” International Journal of Computer Applications October 2012.

[7] P. Agrawal, Varma Gottumukkala, Vaibhav Pandit, and Hailong Li, “Base-station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks,” First IEEE International Workshop on Security and Forensics in Communication Systems, 2012 IEEE.

[8] Priti C. Shahare, Nekita A. Chavhan” An Approach to Secure Sink node’s Location Privacy in Wireless Sensor Networks,“ 2014 Fourth International Conference on Communication Systems and Network Technologies.

[9] Edith C., H. Ngai and Lona Rodhe, “On Providing Location Privacy for Mobile Sinks in Wireless Sensor Networks,” Proc. ACM MSWiM, Oct 2009.

[10] Edith C., H. Ngai,” On providing sink anonymity for wireless sensor networks,” Article first published online: 3 DEC 2010.