Sink Location Privacy Protection in Wireless Sensor Network

Abhishek R. Malviya
Department of Information Technology
MIT College of Engineering,
Pune, India
abhishekmalviya26@gmail.com

Balaso N. Jagdale
Department of Information Technology
MIT College of Engineering,
Pune, India
balasaheb.jagdale@mitcoe.edu.in

***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 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 scheme with attacker node is present in the network and the proposed scheme tries to modify the existing sink location privacy protection scheme by creating zones in the network and analyses the scheme for average throughput, packet delivery ratio, average delay and average energy consumption, normalized routing load and try to resist the traffic analysis attack better.**

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 [1]. Location privacy is extremely important in WSNs. In this paper, we focus on the receiver location privacy in WSN.

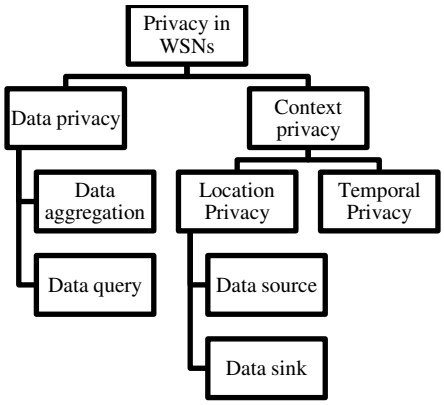

Fig. 1. Classification of privacy in WSN[1].

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 (SLPRP) 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. In Sink Simulation approach explored in [2, 3, 4] 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.

The author proposes the basic routing protocol for sink location privacy called as Location Privacy Routing (LPR) protocol in [5, 6]. 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 [7]. Setting the packet sending rate control between a parent node and its children nodes is the solution to this.

In [8] author proposes a Maximum Amount Shortest Path (MASP) problem which aims to find the optimized mapping between members and sub sinks to minimize the energy consumption under the condition that the total amount of data collected by the mobile sinks [9] is maximized. According to the complexity analysis, it takes long time to calculate the optimal mapping between each member and each sub sink in large scale sensor networks with high density. On the other hand, each member always tries to choose the nearest sub sink as its destination if the constraints about the MReqs are satisfied, which means all members seldom choose the sub sink very far away when all nodes are deployed randomly and uniformly. So the shortest path trees (SPTs) are build based on zone partitioning without relying on geographical information about the sensors and the sinks. Through zone partitioning, the whole monitored area is divided into several zones. And then, the MASP scheme is executed separately to get the optimal assignment of the members to the sub sinks in each zone.

III. PROPOSED SCHEME

Many techniques have been proposed for the location privacy of the sink node in the wireless network. Sink location privacy routing protocol (SLPRP) is one of them.

A. DSR attack affected protocol:

In first step, we are considering the network with malicious or black hole node present in the network. The routing protocol use is DSR protocol and performance parameters are analyzed with varying number of sink.

B. Sink Location Privacy Routing Protocol (SLPRP):

In Second Step, we are using SLPRP scheme[1] for providing sink location privacy with routing protocol as a DSR protocol with malicious or black hole node present in the network and performance parameters is analyzed as a function of number of sink. In SLPRP 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 present in the shortest paths.

C. Zone based Sink Location Privacy Routing Protocol (ZSLPRP):

This paper proposes a modification of the sink location privacy protection scheme in order to improve its performance.

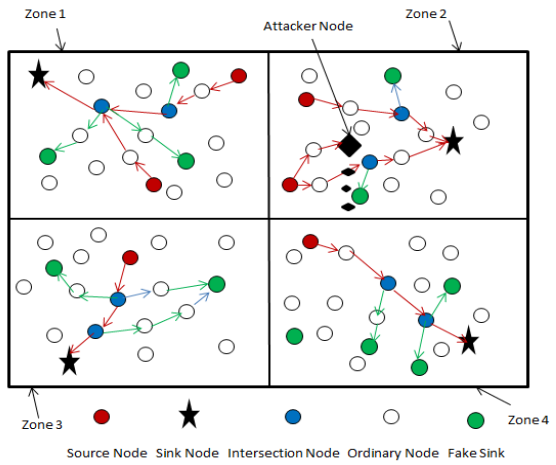

Fig. 2. Scenario of zone based sink location privacy protection scheme.

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 [8] in which the source node belongs to the particular zone send real packet to the sink deployed in that zone. The attacker node is present in the zone 4.
Main objective of using zone routing protocol is:

- To balance energy consumption.
- 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).

Algorithm: Zone based sink location privacy in wireless sensor network.
Start
Step 1: Input wireless sensor network with multiple fake sinks.
Step 2: Divide given area into 'N' number of zones.
Step 3: Set Real Sink Count to one.
Step 4: While Real Sink Count <= 'L'.
Step 5: Every sensor possesses a counter 'C' and a timer 'T', and their initial values are zero.
Step 6: Every sensor receives data from its neighbor nodes in a particular zone.
Step 7: On receiving a packet, every sensor will increase its counter by one.
Step 8: When counter value reaches threshcount 'M' or timer expires, the intersection node will inject fake packets to fake sinks and some random destinations.
Step 9: The intersection node will set its counter and timer zero.
Step 10: Add one to Real Sink Count.
Step 11: End while.
End

IV. SIMULATION RESULTS

We evaluate our scheme performance with NS2 simulations. The simulation settings are summarized in Table 1.

TABLE I. SIMULATION SETTINGS

Parameter	Value
Number of Sensor Nodes	100
Traffic Patterns	CBR (Constant Bit Rate)
Network Size	1000 x 1000
Simulation Time	100 s
MAC Protocol	IEEE 802.11
Routing Protocol	DSR
Number of Sinks	1/2/3/4/5

The topology of the network is generated by uniformly deploying 100 nodes in a 1000 x 1000 m2. In this paper, we consider a WSN with varying sink, and the sink nodes are placed in all over the sensor area. In Table 1, the simulation time is defined as 100 s, during which all transmission takes place with constant reporting rate. In the first step, we only used the simple DSR routing protocol with attacker node placed in the network which is malicious, selfish or faulty node. Which simply drop data, route request or reply packet or drop all packets passing through it, then generate fake reply that shows it has shortest path to the sink. In the second step, we done changes in the routing protocol made it an SLPRP routing protocol, which is the proposed protocol without zone portioning algorithm. In this paper, we compare DSR and SLPRP in terms of performance parameters. In next step, we implement complete proposed scheme with zone partitioning algorithm and compare it with above two protocols, which is out of the scope of this paper.

A. Average Throughput

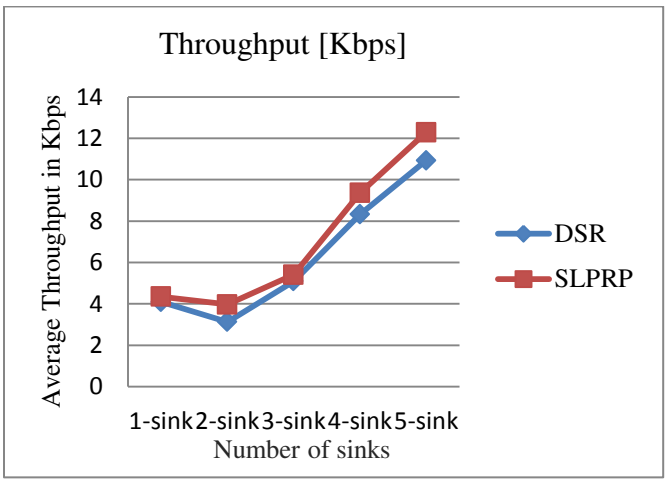

Figure 3. Average Throughput (kbps) as a function of number of sink.

Figure 3 shows that performance of SLPRP is slightly better for the average throughput as compared to DSR. Performance of DSR and SLPRP are increases in average throughput as a function of number of sinks. Due to the hop by hop check by SLPRP increases performance for an average throughput.

B. Packet Delivery Ratio

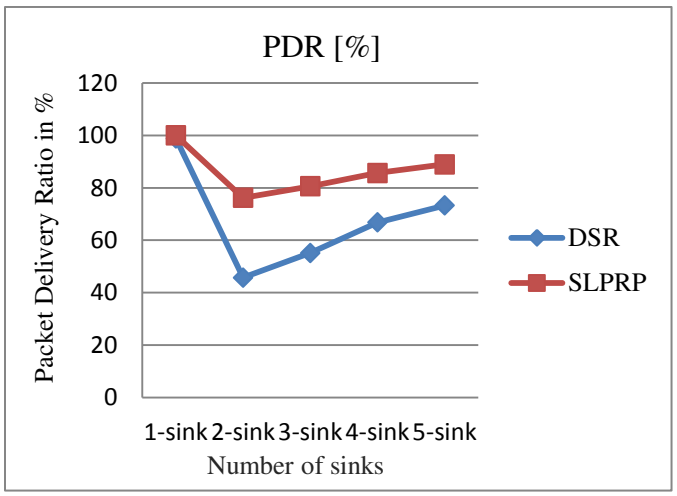

Figure 4. Packet Delivery Ratio (%) as a function of number of sink.

In figure 4 Packet Delivery Ratio is better for SLPRP as compared to DSR. Performance of SLPRP is better for PDR as compared to DSR with varying number of sink. Because SLPRP does the hop by hop packet check during the communication packet dropping rate is decreased within the network.

C. Average End to End Delay

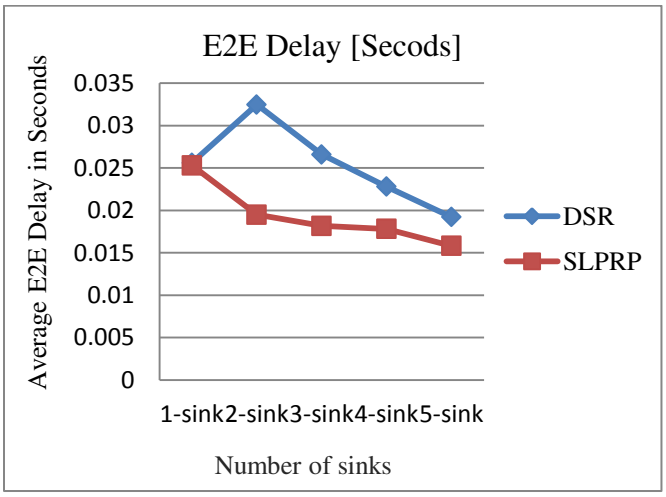

Figure 5. Average Delay (Seconds) as a function of number of sink.

We examine the average end to end delay from the sources to the real sink. Performance of the SLPRP is better for average delay compared to DSR (Refer figure 5). With less number of sink, the DSR gives very poor performance, but with SLPRP the average delay decreases linearly with the increasing number of sink. Because with varying sink packet send to the nearest sink.

D. Average Energy Consumption

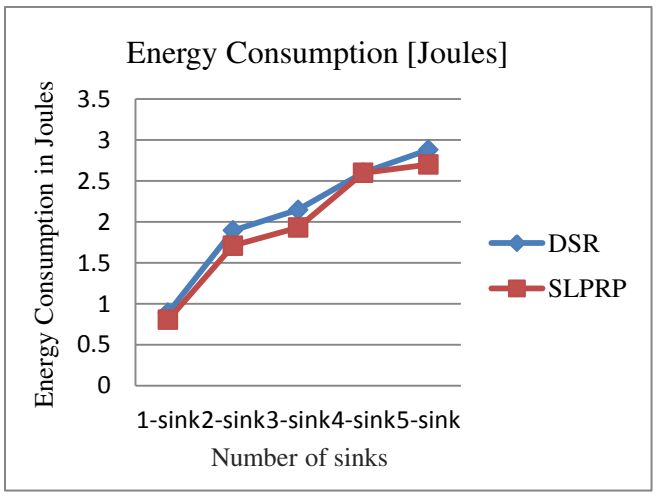

Figure 6. Average Energy Consumption (Joules) as a function of number of sink.

Average energy consumption increases drastically in both DSR and SLPRP with the varying number of sink (In figure 6).In both the protocol the average energy consumption increases because in both the scenario the attacker node is present which drop the packet or generate fake reply packet in response to the route request packet.

E. Normalized Routing Load

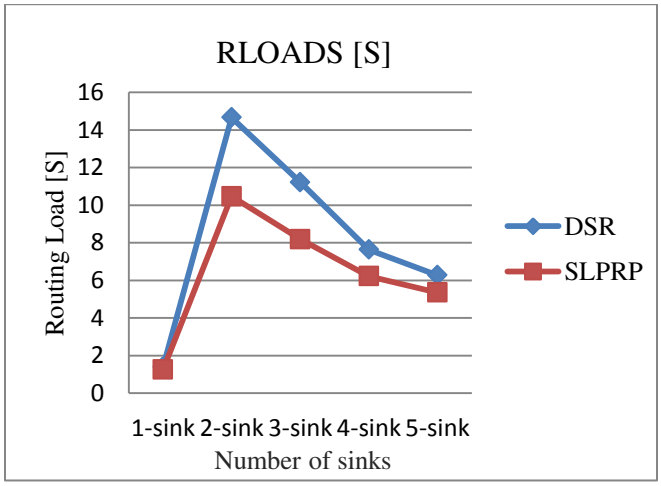

Figure 7. Normalized Routing Load as a function of number of sink.

Figure 7 shows that performance of SLPRP is slightly better

for normalized routing load as compared to DSR. The routing load drastically increases for both DSR and SLPRP up to some threshold point and then decreases linearly with increasing number of sink.

V. CONCLUSION AND FUTURE WORK

In this paper, we analyzed the DSR and SLPRP protocol. We first created the attack affected simulation environment using DSR protocol. We are added different attack as a malicious node, the selfish node or faulty node present in the network. Second, we are using SLPRP protocol to overcome attack affected simulation and improve their network performance. Simulation results demonstrate that the DSR performs poorly for packet delivery ratio and average delay when attacker node presents in the network for MAC 802.11. SLPRP give slightly better performance than DSR. Due to the hop by hop check done by the SLPRP the packet drop done by the attackers is decreased so the packet delivery ratio is increased compared to DSR which only send the packet on the shortest path.

In future work we try to implement the zone based sink location privacy routing protocol (ZSLPRP) and compare it with DSR and SLPRP by analyzing performance parameters like average throughput, average end to end delay, packet delivery ratio and average energy consumption.

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] 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.

[3] 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.

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

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

[6] 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.

[7] Bi Di Ying, Dimitrios Makrakis and Hussein T Mouftah ,“Anti-traffic analysis attack for location privacy in WSNs,” EURASIP Journal on Wireless Communications and Networking 2014.

[8] Shuai Gao, Hongke Zhang and Sajal K. Das,” Efficient Data Collection in Wireless Sensor Networks with Path-Constrained Mobile Sinks” IEEE Transaction on Mobile Computing, Vol. 10, NO. 5, April 2011.

[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.