Protection of Source and Sink in Wireless Sensor Networks

Prabhjot Kaur
Research Scholar, Department of Computer science and engineering
GIMET, Amritsar, Punjab India

Mandeep Kaur
Lecturer, Computer science and technology,
GIMET,Amritsar, Punjab India

ABSTRACT
The deliberation of interloper is to interrupt the communication or to invade the location of sender and receiver. One of the primary concerns of wireless sensor networks is the privacy of sender and receiver. There is always a threat of eavesdropper. The chief objective of this paper is to achieve a high degree of security for both source and sink. Due to an open characteristic of wireless sensor network an adversary can easily detect the location of source or sink by eavesdropping on the sensor nodes. In this paper four protection schemes are discussed that can protect the location of both sink and source. These schemes are forward random walk, bidirectional tree scheme, dynamic bidirectional tree scheme and zigzag bidirectional tree scheme. Also in this paper problems associated with both these scheme are also discussed

Keywords
Wireless, Source, Sink, Eavesdropper, Tree, Privacy

1. INTRODUCTION
Wireless sensor networks consist of numerous small nodes that collect and spread the information for many different types of applications. In wireless sensor network the message or packet goes from sender to receiver via fixed path. The path consists of various nodes and there is a source which sends the information or packet and on other side there is a sink which receives the message. But the main demerit of wireless sensor network is that, any third person or adversary can locate the location of source or sink or both by retracing that path from where message has been sent. Therefore location privacy is a cause of concern for the sender or for the person or organization which is using wireless sensor networks for the purpose of communication. The common techniques used to prevent this problem used are: encryption [2] and authentication [2].

The proliferation of always on WSNs has been accompanied by an attendant loss of privacy, our movements can be silently traced by an eavesdropper [1] who observes the location of source and sink [7]. In either case, they may involve threats to one of the following two types of wireless sensor network privacy content privacy and contextual privacy [1]. Location privacy is strictly needed in order to prevent the adversary from getting the location of any either source or sink[7]. Location privacy is thus very important, especially in hostile environments. There is a strong need to put concentration on protection of our source and sink location from the eavesdropper [1].

To illustrate, how our location becomes visible to the adversary, we consider a habitat monitoring application called ‘‘Panda-Hunter’’ [8] as shown in Fig. 1, in which a typical WSN is deployed to monitor the appearance of the pandas in the forest. There is a central controller (sink in Fig. 1) and several pandas in the monitoring field. The sensor nodes which detect the appearance of the pandas will act as source nodes and will send the monitoring packets to the central controller via multi-hop wireless communications. The central controller can then analyze the life habit of the pandas after receiving the monitoring packets or further send the data to a powerful computer for more complex analysis. This is definitely not safe as the hunter can easily access the location of panda by retracing the path in wireless sensor networks, and can do attack on the pandas. The main issue here is to protect the location of source and sink rather than only source or sink, so, there is strong need of any scheme to protect both the ends effectively. Thus, the end-to-end location privacy protection is a crucial privacy problem in WSNs.

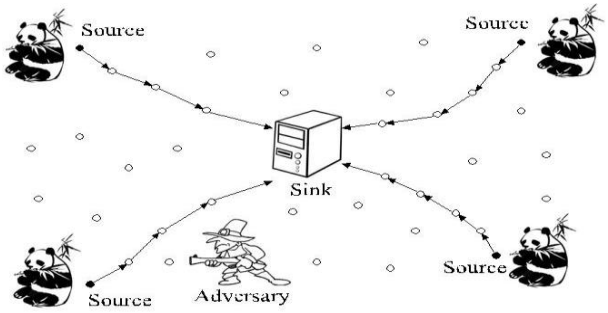

Fig 1: End-to-end location privacy threat [1]

In this paper, we analyze four end-to-end location privacy protection schemes which were introduced to protect both the ends, which can protect against local eavesdropper that might break the location privacy of a source or sink, i.e., the end-to-end location privacy.In this paper we have used word eavesdropper and adversary for thr person who is attacker. The already proposed four location privacy protection schemes are called forward random walk (FRW),bidirectional tree (BT),dynamic bidirectional tree scheme(DBT) and zigzag bidirectional tree scheme respectively. In the forward random walk scheme, every node relays a received packet to a node randomly chosen from its forward neighbors whose hop count to the sink is not larger than its own. To enhance the location privacy of the source and sink, a tree topology is employed at the two ends of the delivery path respectively in the bidirectional tree scheme. In the dynamic bidirectional tree scheme, branches of the trees are generated dynamically to further improve the performance. Lastly, in zigzag bidirectional tree scheme two proxy servers are added which act as source and sink for the adversary and can distract the

eavesdropper from original source and sink as the proxy source and sink will act like original source and sink.

2. FORWARD RANDOM WALK SCHEME

The main problem with wireless sensor network is that the message is delivered along the fixed path so, if we are delivering our packets via fixed path then it is actually become very easy for adversary to trace the path. Therefore the scheme forward random walk is applied to confuse the attacker. In this scheme the random nodes are used for transfer of packets instead of using fixed path a zigzag pattern is used so that adversary will not able to trace the path easily.

In the FRW scheme, a forward random path is employed, which makes it difficult for the adversary to follow the packets' delivery path to capture the source or sink. Considering that a packet is currently held by node i whose hop count to the sink is H_i, the expected number of hops for this packet to be delivered to the sink, denoted as xH_i , can be calculated by the following equation:

$$xH_i = 1 + xH_i - 1\lambda H_i + xH_i\,(1 - \lambda H_i),[1]$$

Here λH_i presents the probability that the packet is forwarded from a node whose hop count to the sink is Hi to a node in its closer list.

In this scheme, three different approaches are used which have their own value:

In first approach the random path has been chosen to distract the adversary and the sender tries to distract the adversary by using fluctuated path to send the message. In the second approach along with the original query message, the destination releases an advertisement packet that propagates along a randomly chosen direction so that all nodes visited by the advertisement packet obtain and store the target location information. In the third method as the query message is considered to follow the random path or distraction of adversary it is assumed that it consumes more energy because using random path obviously increase the number of nodes and the upsurge of nodes also boosts the energy level which is again not beneficial for us. So to solve this problem a protocol is introduced which is known as lukewarm forwarding protocol[2].Lukewarm protocol is a forwarding protocol in which nodes only use local information about the neighbors in order to save information.

2.1 Lukewarm Forwarding Protocol [2]

The protocol considers that the clocks of the sensors are synchronized. The forwarding protocol basically works on time slots as it assumes that every clock is synchronized. Moreover, it requires that the present node which is about to send the packet to next node must be aware about the identity or location of next node so the present node before transferring the packet further must predict the identity of next active node which is known as space look ahead. All the actors like protocol, collisions[2] are predicted in this protocol within one time slot because this protocol works on time slots to save energy.

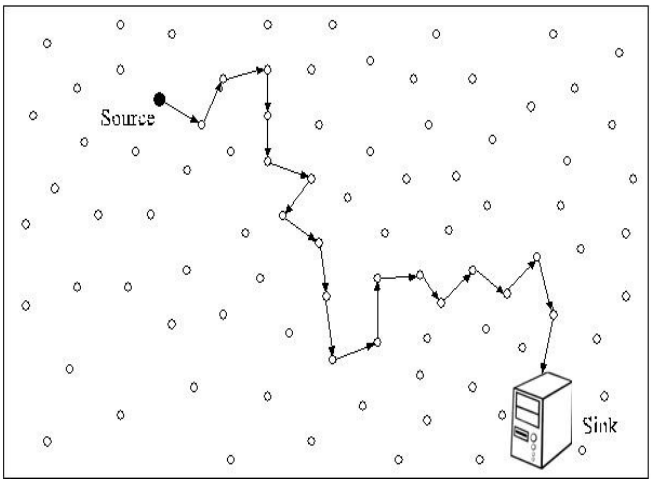

Fig 2: Forward random walk[1]

2.2 Problem with Forward Random Walk Scheme

Although this technique is easy to apply but still it has some flaws. The FRW scheme protects the end-to-end location privacy by randomizing the delivery path. However, it will increase the end-to-end latency i.e. the level of energy consumption is high and it also takes more time to packet get delivered because in fixed path the nodes are less and packet can send in short time but with the increase in nodes the time also get increased. And another demerit of this scheme is that the node is only aware about its neighbors that is one node is only known to its neighbor node as a result the security level is not high in this scheme. The way to improve it is to add dummy message in the network.

3. BIDIRECTIONAL TREE SCHEME

In this scheme, to protect the location of both sender and receiver the branches with nodes are made along with original path just to distract the adversary. The branches are created with the help of dummy messages. As the dummy messages create fake path along with the original one by creating various nodes and give the transverse a shape of tree.

The homogenous routing trees are established which prevent the adversary from interfering in the path of transfer. The main idea is to 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 create the diversionary routes.

The tree topology is introduced to protect the location of sender as well as the receiver in this bidirectional tree scheme. The real messages travel along the shortest path from the source to the sink. To protect the source and sink message is sent through the shortest path but the branches along with that shortest path are created to divert the eavesdropper. When adversary tries to relocate the original path by tracing nodes on which message is travelling it get confused because of the branches created by the he dummy messages and location of source and sink will remain safe.

The real messages travel along the shortest route from the source to the sink node. This approach easily deviate the eavesdropper from the original path.

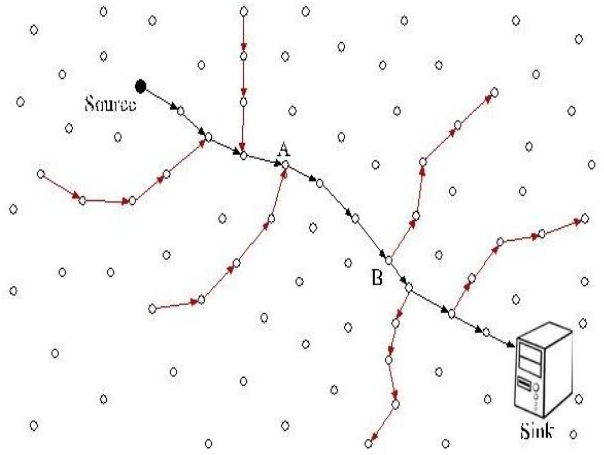

Fig 3: Scenario of bidirectional tree scheme[1]

Similar approach is applied for both the source and sink. Branches are created by dummy messages on both source side and sink side. By adopting this message on both the sides location can be protected.

3.1 Problems with Bidirectional Tree Scheme

No doubt it is a very well scheme to protect both the ends by creating the braches on both ends but there may chances that the adversary may apply some smarter scheme and can trace the path by using its smart scheme. Therefore security is not sure in this scheme. It is possible to distract the adversary by using this scheme but the smart adversary may find out the location from the visible path which is possible if the adversary apply a smarter scheme. Adversary is able to get the path by travelling simply from source to sink or sink to source if it is aware of the use of braches in the network, it can avoid the branches and can travel straight from source to sink and similar it can adopt to travel along sink to source.

4. DYNAMIC BIDIRECTIONAL TREE SCHEM

In dynamic bidirectional tree (DBT) scheme, branches of the trees are generated dynamically to further improve the performance. These branches are to distract the adversary from the original path.

To stop the adversary from getting the source and sink location dynamic bidirectional tree scheme is introduced. Basically this scheme is combination of previous two schemes i.e. forward random walk scheme and bidirectional tree scheme.

Dynamic bidirectional tree not only follows a random path to deliver messages but it also create branches along with that path so that if the adversary tries to retrace its path firstly it get confused by different branches and if he use smart technique and he found the path then it will definitely get distracted by the random path.

In the DBT scheme, real messages are delivered by using the shortest path but the branches are created for the purpose of confusion of eavesdropper.

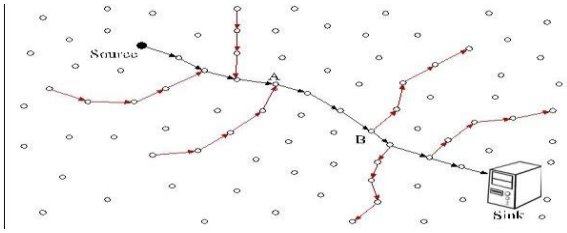

Fig 4: Scenario of dynamic bidirectional tree[1]

4.1 Problems with Dynamic Bidirectional Tree

Just like other schemes dynamic bidirectional tree also has some demerits which prevents it from the proper working. As in this scheme original message and fake message travel in nodes so sometimes it may cause flooding which further results into traffic congestion and the delivery time may be multiplies. This scheme has another drawback that its nodes have to remain active every time because these have to receive packets periodically and packets can be original or fake.

5. ZIGZAG BIDIRECTIONAL TREE SCHEME

The zigzag bidirectional tree scheme (ZBT) is another strong location privacy protection scheme which protects the location of both sink and source.

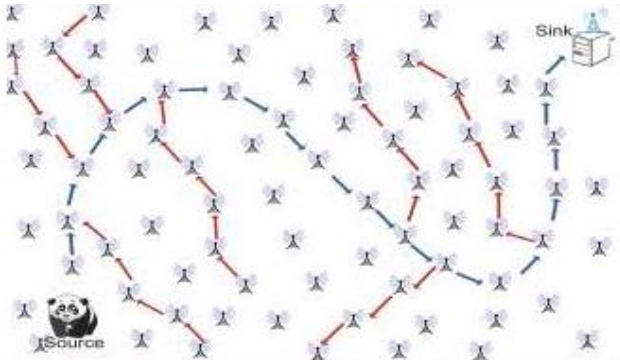

Fig 5.:Scenario of Zig-zag bidirectional tree scheme[8]

In the ZBT, the proxy source and the proxy sink are added between the source and sink. The message travel in three segments which are:

(i) From the source to the proxy source,

(ii) From the proxy source to the proxy sink,

(iii) From the proxy sink to the real sink.

In this scheme the adversary considers the proxy source as original source and the proxy sink as original sink. By considering the proxy servers as sink and source the adversary will attack on proxy server and proxy sink results in protection of original sender and receiver.It is very effective technique for protection of source and sink.

5.1 Problems with Zigzag Bidirectional Tree

As the zigzag routing will be invalid if the proxy sink is close to the source, and it is also compulsory that proxy source will also away from the sink in case of failure this technique will not work. There is always a problem of appropriate distance between source and proxy sink so that eavesdropper cannot detect the exact location o original source, which is possible in case if proxy sink is present near to the original source. Another con of this technique is that it consumes a lot of energy because of more nodes and presence of proxy source and proxy sink.

6. CONCLUSION

The privacy of sender & receiver should be maintained every time data transfer takes place. Intruder always look to interrupt the communication or to invade the location of sender and receiver. The location of both source & sink can be identified easily by eavesdropping. Various schemes are followed in order to protect information from the intruder. In this paper, forward random walk scheme, bidirectional tree scheme, dynamic bidirectional tree scheme and zigzag bidirectional tree scheme has been discussed. In forward random walk scheme, the delivery path is randomized to achieve end to end location privacy. The problem with forward random walk scheme is that, it will increase the end-to-end latency. Furthermore, the FRW scheme relays the packets only to the neighbors in the forward list, resulting in that the safety period cannot be very high. In bidirectional tree scheme the strategy is to create diversionary 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. In dynamic bidirectional tree scheme branches are introduced to confuse the eavesdropper but its hop count is more due to presence f number of nodes. Last zigzag bidirectional tree scheme uses proxy source and proxy sink, but the energy consumption is very high in this scheme.

7. ACKNOWLEDGEMENT

I highly grateful to the Director, Global Institute of Management and Emerging Technologies for providing this opportunity to carry out the present work. I am also thankful to Ms. Mandeep Kaur (Assistant Professor in Computer science department, GIMET) who has been of great help in conclusion of present work.

8. REFERENCES

[1] Honglong chen and Wei lou, "On protecting end to end location privacy against local eavesdropper in wireless sensor networks", *Pervasive and mobile computing*, 2012, Vol. 30.

[2] Chin-fan hsin and Mingyan liu, "Hitting time analysis fo a class of rndom packet forwarding schemes in ad hoc networks", *science direct*, 11 july 2008, Vol. 7, pp. 500-513.

[3] Kavita D, hanabaratti and Rashmi Jodand, "Design of an efficient rndom walk routing protocol for wireless sensor networks", *International Journal of Electronics and Communication Technology*, 2011, Vol. 2,Issue 4 pp.95-98.

[4] Ning wang and George Pavlou, "Scalable sender access control for didirectional multicast routing", Science direct**,** 2003, pp. 539-555.

[5] Samson Raja T, S.Satheesbabu. and Dr. K.Balasubadra, "Bidirectional location privacy scheme against internaladversary in ireless sensor networks", *International Journal of Science and research*, 2014, Vol. 3,Issue 11, pp. 2611-2615.

[6] Pavitha N and S.N. Shelke, "Protecting source and sink node's location against adversaries in sensor network", *International journal of engineering research and general science*, 2014, Vol. 2,Issue 4, pp. 319-325.

[7] Jun Long, Mainxiong ong, Kroo otc and Anfeng liu, "Achieving source location privacy and network lifetime maximization through tree based diversionary routing in wireless sensor networks", *Proc. IEEE*, 2014, Vol. 2, pp. 633-651.

[8] Deewakar Samajdar and Toran Verma, "A Survey on location privacy in wireless sensor natworks",Journal of Emerging Technologies and Innovative Research (JETIR), March 2015, Volume 2, Issue 3,pp.623-627.