A SURVEY ON LOCATION PRIVACY IN WIRELESS SENSOR NETWORK

[1]Deewakar Samajdar, [2]Toran Verma
[1]Research Scholar (M-Tech), [2]Assistant Professor
Computer Science & Engineering Department,
[1]Rungta College of Engineering & Technology, Bhilai, India

***Abstract*— Wireless device Network (WSN) is basically arrangement of distinct and dedicated sensors for observation and recording the healthiness of the surroundings and organizing the collected information at a central location. While several protocols for detector network security offer confidentiality for the content of messages, discourse info typically remains exposed. To conserve user location privacy, spatial and temporal cloaking techniques are the foremost ordinarily used technique in Location based mostly Services. Existing techniques defend the leakage of location data from a restricted opponent who will solely observe network traffic in a very tiny region. In previous papers, it was addressed the importance of location privacy of both the source and sink and propose four schemes called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper. Through analysis and simulation, we tend to demonstrate that the suggested techniques are efficient and effective for source location privacy in sensor networks.**

Keywords—Wireless sensor network, Confused Node, Source simulation

I. INTRODUCTION

Wireless device Network (WSN) is basically arrangement of distinct and dedicated sensors for observation and recording the healthiness of the surroundings and organizing the collected information at a central location . While several protocols for detector network security offer confidentiality for the content of messages, discourse info typically remains exposed. To conserve user location privacy, spatial and temporal cloaking techniques are the foremost ordinarily used technique in Location based mostly Services.

Sensor networks are often used in applications where it is difficult or infeasible to set up wired networks like wildlife habitat monitoring [10], environment monitoring [8], security and military surveillance [9], and target tracking.

Due to open characteristics of wireless communications, it is not hard to attack WSNs with the goal of either obtaining confidential data or simply interrupting the normal procedures of the WSNs applications. In either case, they will involve threats to at least one of the subsequent two styles of WSN privacy, content privacy and discourse privacy.

Panda Hunter Scenarios is proposed in [11], which is Source simulation privacy and Sink simulation privacy technique. In Source simulation privacy technique it hides the location of the source and in Sink simulation technique it creates the vogues/fake path so that the eavesdropper has confused to detect the actual location of panda. Use of Source and sink privacy techniques formalized the location privacy issues under a global eavesdropper and estimated the minimum average communication overhead needed to achieve the given level of privacy.

Confused area method is proposed in [2], to preserve sensor location information in wireless sensor networks. The confused areas consist of a given number of sensor nodes in wireless sensor network. Sensors which are located on each initial area will serve as the receptors. And each sensor will store its neighbors in the same area. Confused Areas method can efficiently protect the location information of the source nodes and the base station.

Walk Scheme Methods is proposed by [3], which it has evaluated the performance in terms Of safety period, end-to-end latency and energy consumption. The simulation results illustrate that the proposed location Privacy protection schemes can obtain satisfied performance.

For example, in the Panda-Hunter Scenario [5], a sensor network is distributed to track endangered pandas. Each panda is associated with a sensor tag that emits signal that can be detected by the sensors in the networks. A sensor that detects the signal is source sensor that sends the location of the panda with the help of intermediate sensors.

In this paper, it is proposed the modified source simulation technique in which the solution is written in terms of a single layer potential over an internal surface through which we make the confusing node and we confuse the hunter by making this node. By this confusing node the hunter will never get the exact location of the panda.

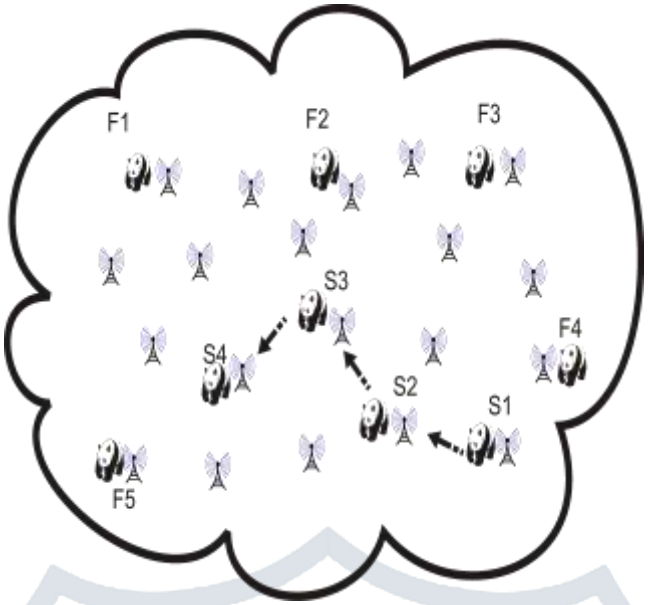

Fig: 1-**Movement Pattern Leaks Location Information.**

The rest of the paper is organized as follows: Section 2 reviews problem statement that describes the problem that in this paper, it generates the fake packet in the sensor network. Section 3 presents the proposed methodology in which we are going to use modified source simulation technique for privacy issues in sensor networks. In Section 4 we discuss the result of the paper where we are going to display that how the modified source simulation technique is better than source simulation technique. Finally, Section 5 concludes this paper and points out some directions for future approach.
Estimated the minimum average communication overhead needed to achieve the given level of privacy.

II. PROBLEM STATEMENT

Location Privacy-
Privacy of location data is regarding dominant access to the current data. We have a tendency to don't essentially want to prevent all access—because some applications will use this data to supply helpful services—but need to be on top of things.

We consider a WSN-based monitoring system called ‘‘Panda-Hunter’’ as shown in Fig. 1, which describes the behavior of fake objects is modeled inaccurately as remaining in one location all the time. Based on this model, the candidate traces are created at locations {F1; F2; . . . ; F6}. Sensors at each of these locations will send fake traffic to the sink, simulating a real object. However, the adversary can simply notice that the object moves around in the field along the path {S1; S2; S3; S4} and use this extra knowledge to distinguish real objects from fake ones.

In this system, we are going to describe that we are making the fake node to confuse the eavesdropper so that the eavesdropper will never get the exact position of the panda and can never be able to hunt the panda.

III. METHODOLOGY

In previous papers, we studied that five methods are used for location privacy protection schemes:-

1. Forward random walk (FRW)
2. Bidirectional tree (BT)
3. Dynamic bidirectional tree (DBT)
4. Zigzag bidirectional tree (ZBT)
5. Location Privacy

1. ***In forward random walk (FRW)*** 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 anonymity of the source and sink, a tree topology is employed at the two ends of the delivery path respectively in the bidirectional tree scheme.

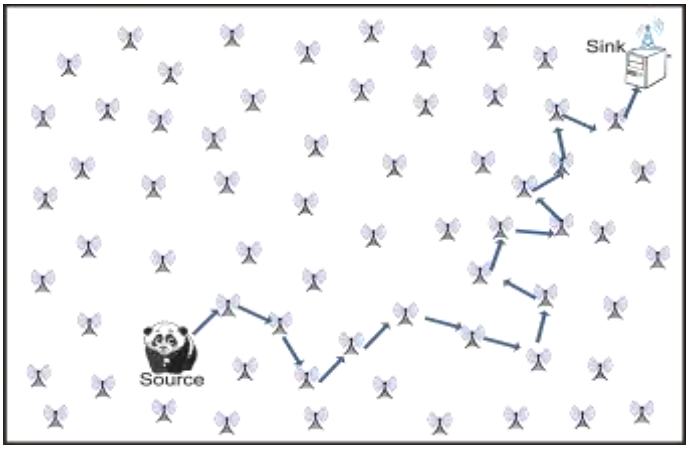

Fig: 2 Forward Random Walk Scheme

2. In ***Bidirectional tree (BT)*** scheme, real messages are delivered along the shortest path, making it possible f or the Eavesdropper to infer the location of the source or sink by extending the line of the shortest path.

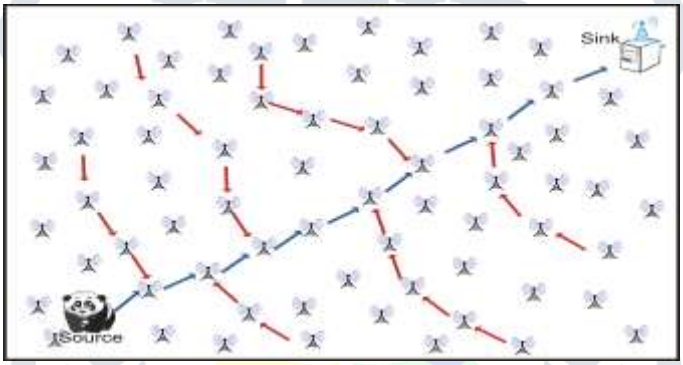

Fig: 3 Bidirectional Tree Scheme

3. In dynamic bidirectional tree (DBT) scheme, branches of the trees are generated dynamically to further improve the performance.

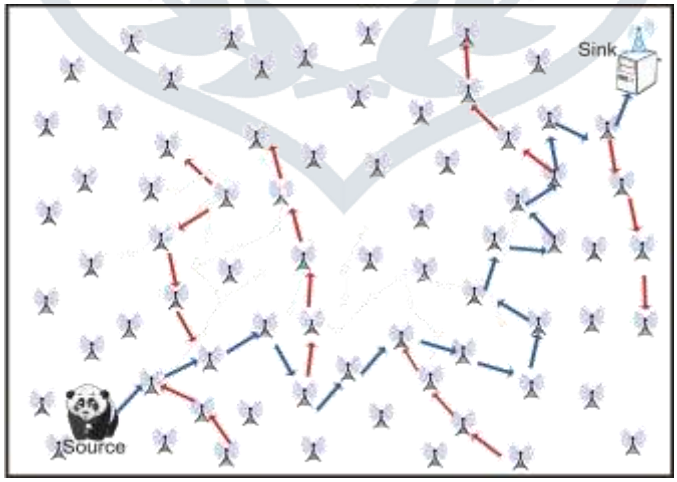

Fig 4 Dynamic Bidirectional Tree Scheme

4. ***Zig-zag bidirectional tree (ZBT)*** scheme is used to prevent the adversary from inferring the direction of the source or sink. Here we employ the proxy source and the proxy sink to
make the real messages be delivered along a zigzag path, which includes three segments: from the source to the proxy source, from the proxy source to the proxy sink and from the proxy sink to the sink.

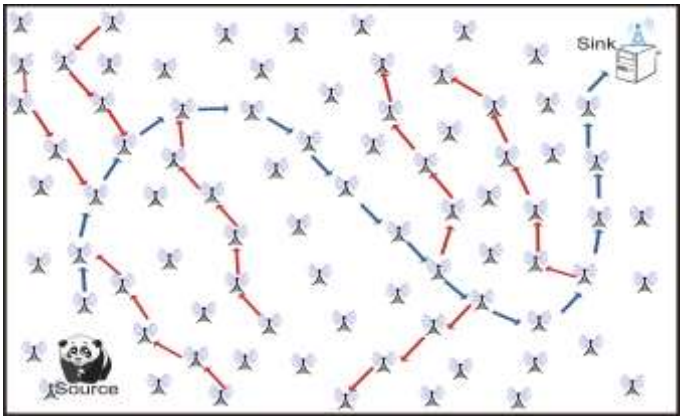

Fig:5 Zig-Zag Bidirectional Tree Scheme

5. In Location Privacy scheme, two techniques are used:

***Source-location privacy**-Source-location privacy is used to secure the location of the source and here it has made the fake source through which various fake packet are generated.

For example: - Panda Hunter Scenario. In this scenario panda is the source and we want to secure the panda from the hunter or eavesdropper. Fake packet generation [1] creates fake sources whenever a sender notifies the sink that it has real data
to send the fake senders are away from the real source and
Approximately at the same distance from the sink as the real sender.

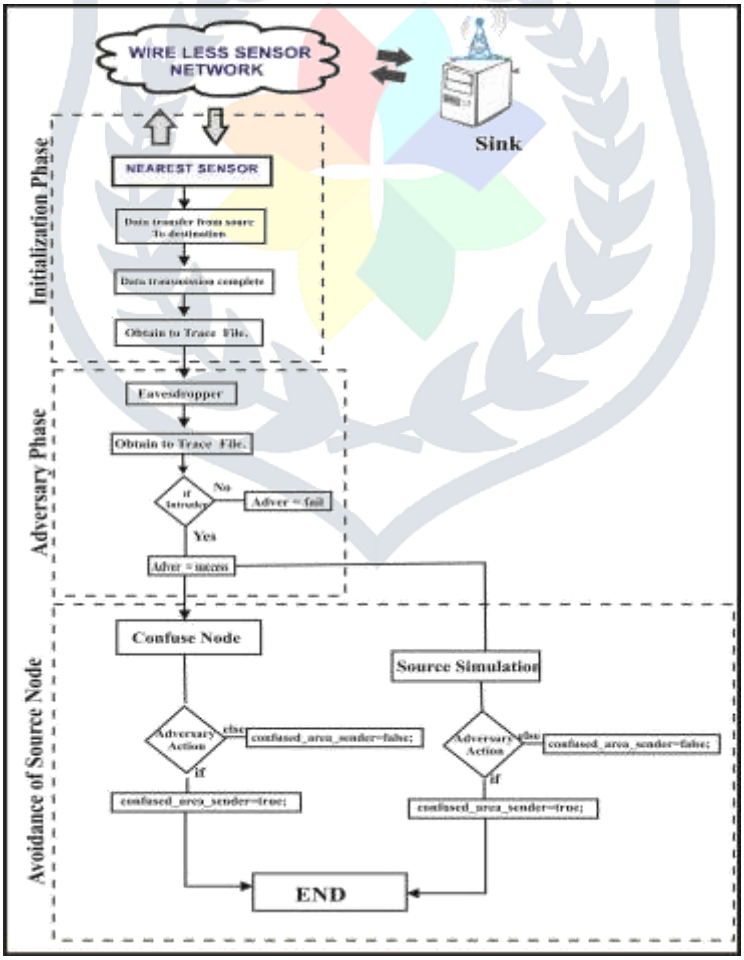

Fig: 6 Flow Diagram of Proposed Methodology

IV. PARAMETERS USED

- **Traffic Data-**Traffic Data is the encapsulated in the data through a network. Traffic Data communication means a computer program generated by a computer system that form a part in the chain of communication, indicating the communication's origin, destination, route, etc.
-**Routing-** Routing is a process of selecting best path in a network.
Routing can be used in two ways-

1. *Forward network traffic*-The packets in the forward network traffic which is delivered to the destination is collecting in the form of node information.
For example- IP Routing is a specific implementation of routing for IP networks.

2. *Backward network traffic*- It is used for updating the routing table. It receives and updates from an interface.

V. CONCLUSION

This paper's objective is to present the major techniques of location privacy. This paper surveys some of the techniques in order from the year 2012 to 2014. The techniques considered in this paper are Forward Random Walk (FRW) scheme, Bidirectional Tree (BT) scheme, Dynamic Bidirectional Tree (DBT) scheme, Zigzag Bidirectional Tree (ZBT) scheme and Location Privacy Strategy. The experimental result show that location privacy with source simulation technique gives excellent result and the rest of the methods also gives the good result but location privacy with source simulation technique gives better result than other methods.

REFERENCES

[1] Kiran Mehta, Donggang Lui and Matthew Wright "Protecting Location Privacy in sensor networks against a global eavesdropper", Published in IEEE 2012.

[2] Liming Zhou, Qiaoyan Wen and Hua Zhang "Protecting sensor location privacy against adversaries in wireless sensor networks", International Conference on Computational and Information Sciences 2013.

[3] Honglong Chen and Wei Lou "On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks", International Conference on Computational and Information Sciences 2014.

[4] Kh Mahmudul Alam, Joarder Kamruzzaman, Gour Karmakar and Manzur Murshed "Dynamic adjustment of sensing range for event coverage in wireless sensor networks", Published in network and computer applications2014.

[5] Stefan K. Starfrace & Nick Antonopoulos "Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks" , Published in Computer Communication 2010.

[6] Tanzima Hashem & Lars Kukik "Don't trust anyone Privacy protection for location-based services", Published in pervasive and mobile computing 2010.

[7] Mohd Fauzi Othmana & Khairunnisa Shazali "Wireless Sensor Network Applications: A Study in Environment Monitoring System", Published in Procedia Engineering 2012.

[8] N.S.Fayed, E.M.Daydamoni and A.Atwan "Efficient combined security system for wireless", Egyptian Informatics journal 2012.

[9] 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

[10] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source LocationPrivacy in Sensor Network Routing ," Proc. Int'l Conf. Distributed Computing Systems (ICDCS,05), June 2005.