IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 7, July 2018

The Stead Fastness Technique for Location Privacy against Local Eavesdropper in Wireless Sensor Network

Amandeep Kaur[1]

E.C.E Department, BGIET, Sangrur[1]

Abstract: Wireless Sensor Network 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. However, due to the open characteristic of wireless communications, an adversary can detect the location of a source or sink and eventually capture them by eavesdropping on the sensor node's transmissions and tracing the packet's trajectories in the networks. The aim of proposed scheme is to provide the source location privacy against hotspot locating attack in Wireless Sensor Network. This thesis provides privacy against the attack by misguiding attacker by sending him the deviated location information and false identity of the sensor nodes through. In the proposed work, the adversary deploys the monitoring nodes in the WSN, here to be referred as attacker in entire work. The proposed schemes on the platform has analyze along with evaluation of performance in terms of safety period, end-to-end latency and energy consumption. The results illustrate that proposed location privacy protection schemes can obtain satisfied performance as proposed schemes has analyze the location privacy protection at the source and sink respectively. The optimal combination schemes are designed to achieve a highest location privacy protection for both ends.

Keywords: Wireless Sensor Network, Location Privacy, Energy Efficiency

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of sensor nodes that are deployed into a large scale-sensing field without a preconfigured infrastructure. The goal of the sensor node is to collect the data at regular intervals, then transform the data into digital signal and finally send the signal to the sink or the base node. Before monitoring the environment, the sensor nodes must identify their neighbor nodes and forms a network. Energy consumption can be takes place while sensing the field and uploading the data to Mobile Collector. The sensor networks can be classified into two types namely, homogeneous and heterogeneous networks. , due to the open characteristic of wireless communications, an adversary can detect the location of a source or sink and eventually capture them by eavesdropping on the sensor node's transmissions and tracing the packet's trajectories in the networks. Thus the location privacy of both the source and sink becomes a critical issue in WSNs. Previous researches only focuses on the location privacy of the source or sink independently. The aim of proposed scheme is to provide the source location privacy against hotspot locating attack in Wireless Sensor Network. This thesis provides privacy against the attack by misguiding attacker by sending him the deviated location information and false identity of the sensor nodes through. In the proposed work, the adversary deploys the monitoring nodes in the WSN, here to be referred as attacker in entire work. The Attacker continuously monitors the traffic of particular area of the entire network. The Attacker collects the traffic information which includes the unique identity of the node, its location (x,y coordinates), time at which the information is last updated and the speed of the mobile node. It collects this information of mobile nodes. On the basis of this information, it attacks the nodes by sending the false reply of route existence from sender to receiver and drops all the data packets. The proposed schemes on the platform has analyze along with evaluation of performance in terms of safety period, end-to-end latency and energy consumption. The results illustrate that proposed location privacy protection schemes can obtain satisfied performance as proposed schemes has analyze the location privacy protection at the source and sink respectively. The optimal combination schemes are designed to achieve a highest location privacy protection for both ends.

II.DATA COLLECTION IN WIRELESS SENSOR NETWORK: A STUDY

In 2015, Deewaker Samajdar et al [1] (**A Survey on Location Privacy in Wireless Sensor Network").** 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 addressed the importance of location privacy of both the source and sink and propose four schemes called Forward Random Walk (FRW), Bidirectional Tree (BT),

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 7, July 2018

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.

In 2015, S.Girija et al [2](" **Performance Analysis of Energy Utilization in Static and Mobility Relaying in WSN").** The work proposes Relative Power Adaptable Distance Aware Routing for the less energy consumption. The relay in the proposed scheme is mobile. Therefore the energy consumption for each node and also the number of relay nodes gets decreased.

In 2014, Honglong Chen et al [3] (**"On Protecting End-to- End Location Privacy against Local eavesdropper in Wireless Sensor Network"**) The proposed work is to address the importance of location privacy of both the source and sink and propose four schemes called forward 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.

In 2015**,** A.Abitha et al [4](**"Efficient Data Gathering With Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks",**) The proposed work used mobile sink to gather the data from sensor nodes to conserve the battery life of network. Again there is a chance of creation of loopholes during the data gathering process. There is a need to detect the loopholes and to correct them. In this paper we use contki algorithm to find loopholes and remove them from the network.

In 2010,Yun Li et al [5](**"Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks"**) This paper proposes source-location privacy schemes through routing to randomly select intermediate node(s) before the message is transmitted to the SINK node. It first describes routing through a single randomly selected intermediate node away from the source node and secondly presents routing through multiple randomly selected intermediate nodes based on angle and quadrant to further improve the global source location privacy.

III. ISSUES IN DATA COLLECTION

- Limited resources.
- Latency, Scalability and Integrity problem.
- There is no re-transmission process.
- It consumes more energy and time.

IV. RESULTS

The whole scheme has been implemented in NS2.35. The comparison was done on the basis of packet delivery ratio and throughput. Packet delivery ration is the percentage of packets successfully delivered in network. Throughput is defined as amount of data received at the base station per unit of time.

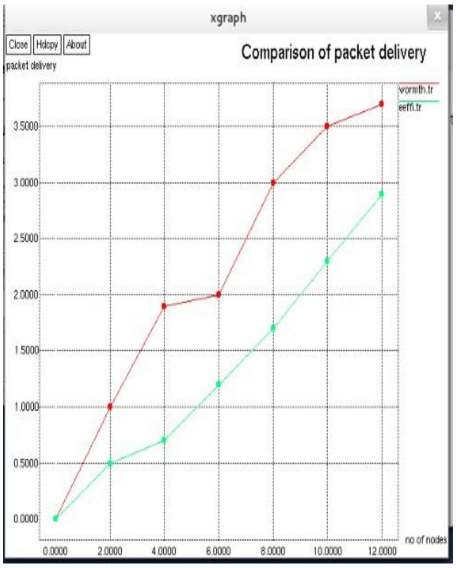

Figure 1: Packet delivery comparison graph

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 7, July 2018

In this Figure shows the end-to-end latency comparison for our proposed scheme and the previous schemes. For the Protocol scheme, as the real messages are delivered along the Protocol from source to sink, they would achieve the shortest end-to-end latency. Since the real messages in the FRW and DBT schemes are delivered along the forward random walk path, the end-to-end latency of these two schemes is similar. Also it is same for BT and ZBT schemes because they follow the shortest path. When the hop count equals to 10, the end-to-end latency of the ZBT scheme is the largest as it employs the zigzag path to mislead the adversary. When the hop count is larger than 15, the end-to-end latency of the FRW and DBT exceeds that of the ZBT scheme.

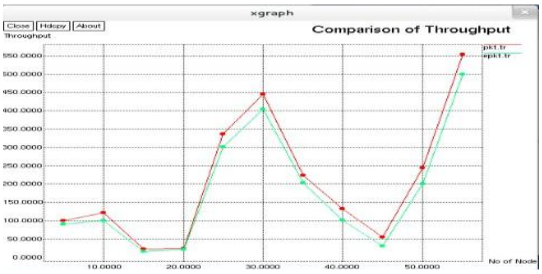

Figure 2: Throughput comparison Graph

In this Figure, the safety period of the sink location privacy of the previous four schemes and our proposed scheme under the cautious adversary model. The Protocol scheme achieves the highest performance while the other scheme has the lowest safety period. As it is more time-consuming for the adversary to capture the sink than the source, the safety period of the sink location privacy is also larger than that of the source location privacy.

V. CONCLUSION

The end-to-end location privacy is an important issue in WSNs. In this we address the necessity of simultaneously protecting the location privacy of both the source and sink in the habitat monitoring system. We propose Protocol Scheme, to deliver messages from source to sink, which can protect the end-to-end location privacy against the local eavesdropper. We also implemented the proposed schemes on the ns-2 platform, and evaluate the performance in terms of safety period, end-to-end latency and energy consumption. The results illustrate that our proposed location privacy protection schemes can obtain satisfied performance, as our proposed schemes have analyzed the location privacy protection at the source and sink respectively. We have designed an optimal combination schemes to achieve a highest location privacy protection for both ends.

REFERENCES

[1] Honglong Chen, Wei Lou.(2007),"On Protecting End-to- End Location Privacy against Local Eavesdropper in Wireless Sensor Network", Elsevier.vol. 16, pp 36-50.

[2] Martin Lukas, Igor Stubailo, Richard Guy, Paul Davis, Victor Aguilar Puruhuaya, Robert Clayton, Deborah Estrin. (2009), "First-Class Meta-Data: A Step Toward Highly Reliable Wireless Eismic Network in Peru" In: Information Processing in Sensor Network, New York, pp 1-8.

[3]Bakhouya. Gaber, M Wack.(2009),"Performance Evaluation of Protocol for Inter-Vehicle Communication", Information Theory and Aerospace & Electronic Systems Technology, Wireless, pp. 289-293.

[4] Rubia, Sivan Arul Selva. (2014), "A Survey on Mobile Data Gathering in Wireless Sensor Network –Bounded Relay", IJETT, Volume 7, pp 205-208

[5] Aarti Arjun Andhale, Prof. B.N. Jagdale. (2014), " Light Weight Security Protocol For Wireless Sensor Network's (WSN)" IJERT, Vol.3, ISSN No- 2278-0181.

[6] G. Uma, A. Dinesh. (2013), "Sequential Based Hypothesis Testing in Wireless Sensor Network" Global Research Analysis",vol.2 Issue 11, ISSN No 2277 –8160.

[7] Adrian Perrig, Robert Szewczyk, J.D. Tygar. (2002), "Security Protocols for Sensor Network", ACM, VOL. 8, Issue 5, pp- 521-534.

[8] M.Narendran, P.Prakasam. (2014), "Mobility Based Energy Utilization in Wireless Sensor Network", IJETCAS, ISSN-2279-0047.

[9] S. Girija, S. Arunmozhi, S. Anbazhagan. (2015), Performance Analysis Of Energy Utilization in Static and Mobility Relaying in WSN", IJSETR, Vol. 4, Issue 3.

[10] A. Abitha, S. Sujatha, A. Stephy. (2014),"Efficient Data Gathering With Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks", IJETT, Vol. 18.

[11] Milan Erdelj. (2013) "Mobile wireless sensor network architecture and Applications to Mobile Sensor Deployment", University Lille 1

[12] Pavitha N, S.N.Shelke,(2014), "Providing Source and Sink Location Privacy Against Eavesdropper in Sensor Networks: a Survey" International Journal of Research, Vol.1, Issue-6.