A Survey Paper on Scalable & Routing Efficient Methods for Source Location Privacy in WSNs

Pallavi S. Patil
PG Student, Department of Computer Engineering,
Sinhgad Technical Education Society's, Smt. Kashibai Navale College of Engineering
Pune, Maharashtra, India

Jyoti N. Nandimath
Asst. Prof. Department of Computer Engineering,
Sinhgad Technical Education Society's, Smt. Kashibai Navale College of Engineering
Pune, Maharashtra, India

***Abstract*— The use of wireless sensor networks (WSNs) in many real time applications are growing significantly due to its wide range of benefits to end users. The major issue with WSNs is the security. Researchers have already presented various methods over WSN security, especially for privacy preservation. From the literature study, the privacy preserving security methods for WSN are having influence over the performance parameters like latency, energy efficiency, communication cost, throughput etc. WSNs are resource constrained, means sensor nodes having limited resources. Most existing methods use the PKI (public key infrastructure) for security purpose, but these methods consume more power of sensor nodes as well as not scalable. Thus to overcome these two limitations, recently the new privacy preservation method is introduced. This method proposed some criteria for the quantitative metrics source location privacy (SLP) for routing oriented methods in WSN. Using this method, the SLP is achieved with goal of efficient energy utilization via the two phase routing. It means SLP through the Routing to a randomly selected intermediate node (RSIN) and a network mixing ring (NMR). However this method is not scalable as required for most of real life applications, as well not evaluated for other performance metrics such as throughput, packet delivery ratio and end to end delay which are vital for any routing scheme in WSN. Therefore in this paper we are presenting the improved method with aim of achieving the network scalability and efficient routing performance while maintaining the source location privacy security.**

Keywords*— Cryptography, public key infrastructure, source location privacy, privacy preservation, energy consumption, scalability, sensor network.

I. INTRODUCTION

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location.

The main characteristics of wireless sensor network include:

- consumption constrains for nodes using batteries Power or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

Sensor networks can be used for wide range of applications where it is difficult or infeasible to set up wired networks. Some of the areas include forest fire detection, air pollution monitoring, health, wildlife habitat monitoring etc. A sensor network can be deployed in a forest to detect the occurrence of fire. The sensors measure the temperature, humidity and gases due to the fire in the woods or vegetation. Wireless sensor networks have been deployed in various cities to detect foreign chemical agents in the air. Sensors are used by the doctors to monitor the physiological condition of patient.

Privacy is one of the major issues in wireless sensor network. Privacy may be categorized into two subclasses: content-oriented privacy and contextual privacy. Content-oriented privacy is concerned with the ability of adversaries to learn the content of transmissions in the sensor network. Contextual privacy concerns the ability of adversaries to infer information from observations of sensors and communications without access to the content of messages. In contrast to content-oriented security, the issue of contextual privacy is concerned with protecting the context associated with the dimensions and transmission of sensed data. For many scenarios, general contextual information surrounding the sensor application, specially the location of the message originator and the base station called as sink, are sensitive and must be protected. Among the different security threats in wireless sensor networks one is eavesdropping which involves attack against the confidentiality of data that is being transmitted across the network. Various privacy-preserving routing techniques have been developed for sensor networks. Most of them are designed to protect against the local eavesdropper and some of them are capable of protecting against global eavesdropper. However many of the methods are suffered from the energy utilization and packet delivery ratio related issues as the scalability of network increases.

Recently we have studied the approach for improving the energy consumption, throughput performance as compared to existing techniques in [1]. This method delivers the best performance for energy consumption and message delivery latency. However for claiming this method efficiency we need to check further its routing performances such as throughput, end to end delay, packet delivery ratio by considering the

network varying scalability. Thus in this paper we are presenting the same using existing methods given in [1].

II. ISSUES IN WIRELESS SENSOR NETWORK

Communication networks require privacy in order to control information related to communication. Wireless sensor networks have some of security and privacy issues discussed below.

A. Security and Privacy issues in WSN

Security issues in wireless networks are different from that of traditional wired networks, mainly because wireless networks are open networks. They are open because the radio medium is a broadcast medium, in which any potential eavesdropper can easily gain access to the data which is transmitted through the network.

Some of the security and privacy issues are :

- Data Confidentiality
- Data Integrity
- Data Authentication
- Monitor and Eavesdropping
- Traffic Analysis

III. LITERATURE SURVEY

In the literature survey we will discuss Source Location Privacy Preserving Schemes for wireless sensor networks: Below in literature we are discussing some of them.

- *Baseline Flooding:* In [2, 3] author has explored the technique of Baseline Flooding in which the source node transmits message to each of its neighbours. These neighbours in turn retransmit the message to each of its neighbours and so on. Thus packet is routed from source to destination through number of paths to make it difficult for an adversary to trace the source. No node in the network retransmits the packet. Adversary can trace the node using backtracking , thus this method does not provide much privacy but consumes significant amount of energy.
- *Single Path Routing:* In [3] author has discussed the Single Path Routing technique in which unlike flooding, the node forwards message only to one of its neighbours. This technique requires pre-configuration phase where sink initiates the flood setting the hop count to zero. The packets from the neighbours are processed only once. Every time the node receives the message the hop count is incremented by one and stored in its local memory. Then the minimum value of the number of hops is selected, accordingly the neighbours are updated. The head of the neighbour list that has shortest distance to the sink is chosen as a path to forward the message to the sink.
- *Routing With Fake Messages*: The next technique that author proposes in [2, 3] is routing with fake messages. In this technique destination creates fake sources whenever a sender notifies the destination that it has real data to send. These fake senders are away from the real source and approximately at the same distance from the destination as the real sender. Both real and fake senders start generating packets at the same time. This scheme provides decent privacy against a local eavesdropper. While implementing this technique author has made certain observations as follows:
  - If the rate of fake message is same as the real message then adversary toggles between real source and fake source and cannot progress towards either of them.
  - If the rate of fake message is less than that of real message then the adversary will be drawn towards real source.
  - If the rate of fake message is greater than that of real message then the adversary will be kept at the real source.
  - Thus injecting fake messages at the faster speed than real message will protect the privacy but will require more energy.
- *Phantom Flooding/ Routing:* In [2, 3] Author proposes the phantom Flooding/ Routing, which achieves location privacy by making every packet generated by a source, walk a random path which is either pure random walk or directed walk which let the messages towards the phantom source. Then the single path routing or flooding is employed to route the message toward the destination. As different messages exhibits different path this algorithm increases the safety period against local eavesdropper but the latency increases because of directing every message to a random location first.
- *Cyclic Entrapment Method:* In [4] author has put forward the Cyclic Entrapment Method that creates looping paths at various places in the sensor network. When message is routed from source to destination each node on a route will check if it is on a loop. If so, it will activate the loop by sending fake message. If an adversary is trying to analyze the route and trace the path towards source, if it finds a node that is common to both loop and the true path then adversary has to make the decision which way to go. This will cause a local adversary to follow these loops repeatedly, if wrong decision is taken and thereby increase the safety period. Energy consumption and privacy provided by this method.
- *Location Privacy Routing Protocol (LPR):* The author in [5] focuses on packet tracing attack and proposes location privacy routing protocol (LPR). In this technique each sensor divides its neighbours into closer list and further list. After the construction of lists sensors select the neighbour as the next hop randomly from either of the two list as a result routing paths from source to destination is not fixed. If sensor selects the next hop from closer list then energy efficiency will be greater and if it selects next hop from the further list, privacy protection will be stronger. The LPR is augmented with fake packet injection so as to minimize the retrieval of traffic direction information by the adversary.
- *Random Data Collection Scheme:* In [6] random data collection scheme is designed to provide location privacy to mobile sinks. It comprises two steps, random data forwarding storage and random Movement of sink in data

collection. In first step whenever 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. This message travels the random path until hop cont field equals the pre-define length of the random path. In second step 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.

- *Greedy Random Walk (GROW):* In [7] author proposes the GROW algorithm for preserving source location privacy in monitoring based wireless sensor networks. Initially sink sets up the random path to receive packets from the source. The source then forwards the packet through the random path until it reaches the sink. Forwarding a packet by sensor to one of its previous hop's neighbour is not beneficial. Bloom filter is used to prevent this case. In the forwarding packet bloom filter stores all the current neighbours. When sensor selects any of its neighbours for packet forwarding, it checks if that neighbour is already in the filter.
- *Source Location Privacy through Routing* to a Random Intermediate Node (RRIN) The author proposes the technique RRIN to achieve source location privacy in wireless sensor network by using the concept of dynamic routing in [8]. In this approach each packet is routed through the node which is selected randomly according to the relative location of the sensor node. The intermediate node should be at least some minimum distance away from the source node in order to avoid the exposure of the source location to the adversary. This scheme is suitable for small scale sensor network.
- *Periodic Collection:* In Periodic collection [11] sensor nodes independently and periodically transmits packets at rational frequency without concerning whether there is real data to send or not. This is because the traffic pattern where the object resides is changed due to the presence of real objects and this change can be easily identified by global eavesdropper. This method provides optimal location privacy but consumes substantial amount of energy and is not suited for real time application.

IV. PROPOSED SYSTEM

The results of the survey shows that there is a broad room for research on preserving location privacy considering various parameters like energy efficiency, latency, security, communication cost. However most of these schemes require public-key cryptosystems and are not suitable for WSNs, because it consumes more energy. Most of methods are not scalable in nature; it means that the performance of these methods decreases as the number of sensor nodes increases. Recently the new method presented in [1] solve the above two main problems more efficiently. The experimental results claims that proposed approach in [1] delivers the best performance as compare to all existing methods in terms of energy consumption and message delivery latency. However these results are not claiming the scalability of this approach as well as other routing parameters such as throughput, end to end delay etc.

Thus in this paper, we further extending the approach presented in [1] by considering the working of network scalability under the different network scenarios and routing performances. Implementing source location privacy makes it possible to hide the location information of the transmitting node. Classified as a contextual privacy protection technique, the source location privacy is an essential feature of those real life sensor networks which have been deployed for monitoring events happening at particular locations. This paper designs a source location privacy scheme using cluster based anonymization and random routing. The privacy measure index is then evaluated in order to estimate the overall privacy achieved by the SLP scheme. The effect of the privacy scheme on end to end message delay is observed, for estimating the network performance degradation and establishing the efficacy of the SLP scheme.

We have considered all the methods and algorithms presented in [1] along with below functionality for improving the scalability.

Our Proposed work is based on two phase routing such as NMI and RSIN as described above. With the use of this we are achieving the efficient energy SLP, and using this process of cluster head binding we achieved the network scalability.

V. CONCLUSION

In this paper we have presented the new method for source location privacy preservation in WSNs. As the sensor network is widely used, it is vulnerable to many security threats, thus privacy preservation techniques are employed by various authors. However the efficiency of such methods is based on routing performance, energy efficiency as well as network scalability. The proposed approach in this project is based on two phase routing such as RSIN and NMI as described above, with the use of this we are achieving the energy efficient SLP.

ACKNOWLEDGMENT

The proposed system is based on IEEE Transaction paper under the title "Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 7, JULY 2012.

REFERENCES

[1] Yun Li, Jian Ren, and Jie Wu "Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 7, JULY 2012.

[2] C.Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy Constrained Sensor Network Routing," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.

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

[4] Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006.

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

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

[7] Yong Xi, Loren Schwiebert and Weisong Shi, "Preserving Source Location Privacy in Monitoring Based Wireless Sensor Networks.

[8] Yun Li and Jein Ren, "Source Location Privacy Through Dynamic Routing in Wireless sensor Network", Proc. IEEE INFOCOM, 2010.

[9] Leron Lightfoot, Yun Li and Jian Rein, "Preserving Source Location Privacy in Wireless sensor Network using Star Routing", Proc. IEEE Globecom, 2010.

[10] Yi Ouyang, Zhengyi Le, Donggang Liu, James Ford, Fillia Makedon, " Source Location Privacy against Laptop–Class Attacks in Sensor Networks", Proc. ACM SecureComm, Sept. 2008.

[11] Yi Ouyang, Zhengyi Le, Donggang Liu, James Ford, Fillia Makedon, " Source Location Privacy against Laptop–Class Attacks in Sensor Networks", Proc. ACM SecureComm, Sept. 2008.