ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Routing Efficient Method for Preserving Source Anonymity In Wireless Sensor Networks

Pallavi S. Patil
PG Student M.E, Computer Dept,
Smt. Kashibai Navale College of Engineering,
Pune, Maharashtra, India

Prof. J. N. Nandimath
Assistant Professor, Computer Dept
Smt. Kashibai Navale College of Engineering,
Pune, Maharashtra, India

***Abstract:*** The emerging field of Wireless Sensor Networks combines computation, sensing , computation and communication into a single and tiny device. However, providing location privacy in a WSN is a challenging task. An adversary can easily intercept the network traffic due to the use of the broadcast nature of transmission. It can then perform traffic analysis and identify the source sensor that initiates the communication with the Base Station. 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:*** Ranked Cryptography; public key infrastructure; source location privacy; privacy preservation; sensor network ; NMR.

## I. INTRODUCTION

A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or an information technology (IT) framework. They 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.

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. RELATED WORK

### A. *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.

*Single Path Routing:* In [2] 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.

*Baseline Flooding:* In [2, 3] author has explored the technique of Baseline Flooding where 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.

*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. 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 [10] 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.

### B. *Motivation:*

The main task of wireless sensor nodes is to sense and collect data from a target domain, process the data, and transmit the information back to the specific sites where the underlying application resides. Achieving this task efficiently requires the development of an energy-efficient routing protocol to set up paths between sensor nodes as well as preserving source anonymity in the WSN is equally important .The path selection must be such that the lifetime of the network is maximized and location privacy for the sensor node should be achieved.

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. Proposed method for source location privacy tries to solve many issues and provides better security.

.

## III. PROPOSED APPROACH FRAMEWORK AND DESIGN

### A. *Problem Defination*

Development of Secure and Efficient method for preserving source anonymity in the WSN is challenging and checking previous methods with the perspective of energy efficiency, latency, security, communication cost is also a difficult work.

We will check the existing method for such parameters and will try to solve some issues.

### B. *Proposed system and Design*

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 [11].

Sensor Node: A sensor node, also known as a mote (chiefly in North America), is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network.

Message Unique ID: We present a distributed algorithm that assigns globally unique IDs to sensor nodes. Initially, we assume that all nodes are awake during the execution of the algorithm. This assumption is relaxed later in this paper to accommodate a dynamic network where nodes can join the network at any time during the initial execution of the algorithm or after its termination. The objective is to assign temporary unique identifiers in the form of potentially long vectors of bytes. A tree structure rooted at the node initiating the algorithm is established during this phase. The main here is to guarantee the uniqueness of the assigned IDs and to minimize cost by controlling the probability of message collisions.

Key Management: Key Management includes the processes of key setup, the initial distribution of keys and key revocation (removal of the compromised key). Many Security-critical applications that depend on key management processes demand a high level of fault tolerance when a node is compromised.

Three keying models are used to compare the different relationships between

WSN Security and operational requirements; we require two kinds of keys in our scheme:

Grid-key $KG_i$: the key shared between grid $G_i$ and the SINK node.

Ring-key KAB: the key shared between ring grid A and ring grid B.

The grid-keys are used to provide message content confidentiality. When the $i_{th}$ normal grid has a message m to transmit, the message is first encrypted using the grid key: $KG_i$ , then its dynamic ID $id_{ij}$ j is prefixed to the encrypted message. Therefore, MSG = $ID_j^{(i)}$ || $EK_{gi}(m)$ will be transmitted from the source node to the SINK node, where EKGi is the cipher text of m, encrypted using the secret key KGi shared between the $i_{th}$ grid with dynamic $ID_j^{(i)}$ j and the SINK node.

Cluster head binding: Cluster head binding (CH) is server head on one side of the head. It is used for scalability improvement.

Two Phase Routing: a two-phase routing. In the first routing phase, the message source randomly selects an intermediate node in the sensor domain and then transmits the message to the randomly selected intermediate node (RSIN). This phase provides SLP with a high local degree. In the second routing phase, the messages will be routed to a ring node where the messages will be blended through a network mixing ring (NMR).

RSIN: As described before, phantom routing has no control over the phantom source without leaking significant side

information. The message source first randomly selects an intermediate node at the sensor domain based on the relative location of the sensor node.

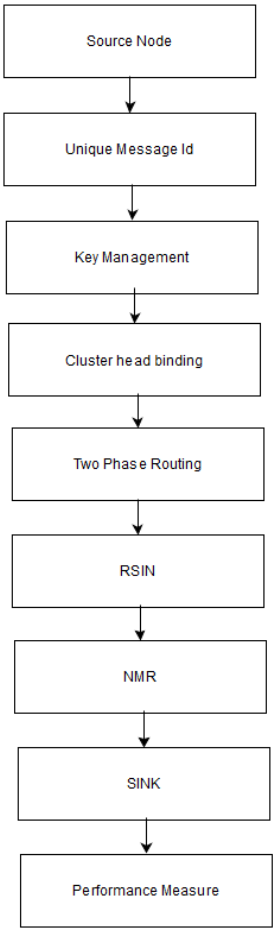


**Fig 1: System Flow**

SINK: Message should be sent at a rate which can ensure that all the messages are embedded in vehicle messages and forwarded to the SINK with minimum delay.
NMR: In the second routing phase, the messages will be forwarded hop-by-hop in the mixing ring. The network mixing ring is a logic ring established by selecting a set of hop-by-hop connected grids that can form a ring. The ring nodes can be either regular nodes or special nodes. In the case that the ring nodes are regular nodes, the ring nodes in the selected grid can take turn to be the ring node to achieve energy balance.
RSIN: As described before, phantom routing has no control over the phantom source without leaking significant side information. The message source first randomly selects an intermediate node at the sensor domain based on the relative location of the sensor node.
SINK: Message should be sent at a rate which can ensure that all the messages are embedded in vehicle messages and forwarded to the SINK with minimum delay.

### *C. Notations and Proposed Mathematic*

The message is first transmitted from sensor node to the randomly selected intermediate node. For this the random distance is calculated as $d_{rand}$ and intermediate node is selected.

*Notations:*

An asset monitoring WSN is a six-tuple (N; S; A; R; H; M), where

1. N = {ni}iεI is the network of sensor nodes ni, which are indexed using an index set I.

2. S is the network sink, to which all communication in the sensor network must ultimately be routed to.

3. A is an asset that the sensor network monitors. Assets are characterized by the mobility pattern that they follow.

4. R is the routing policy employed by the sensors to protect the asset from being acquired or tracked by the hunter H.

5. H is the hunter, or adversary, who seeks to acquire or capture the asset A through a set of movement rules M.

In the routing policy R,

- Safety Period (Φ) is the number of new messages initiated by the source node that is monitoring an asset, before the adversary locates the asset.
- The capture likelihood (L) of a routing protocol R for a given adversarial movement strategy M is the probability that the adversary can capture the asset within a specified time period.

*Proposal Mathematical:*
Input
$N = \{N_i\}$
$H=\{H_i\}$
Intermediate Result
R = {N}
Output
S = Sink

### *D. Evaluation of result*

In this section we discussed the results based on graphs. If an adversary tries to track the message back to the source location from the message in the route path through which the packet is being transmitted to the SINK node. To the best extend, the adversaries will be led to the randomly selected intermediate node, instead of the actual message source.
Since the intermediate node is randomly selected for each message, the probability that the adversaries will receive the messages from one source node continuously is negligible.

The number of dead and half alive nodes is calculated. The proposed algorithm is having highest Half alive nodes which shows that we can efficiently route the messages to achieve global source location privacy with energy efficiency. Figure 2 shows the dead node comparison.

The energy required for the communication between sensor nodes is calculated and figure 3 shows that the proposed algorithm uses the minimum energy for the communication

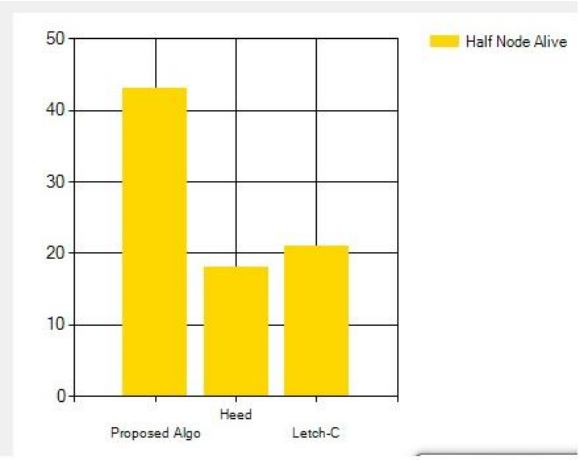


Figure 2 : Graph showing comparison of Half Alive Nodes in the system

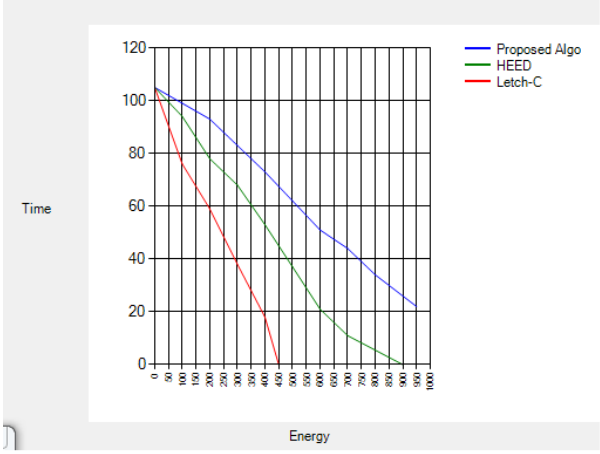


Figure 3 : Graph showing Comparison of energy used

## IV. CONCLUSION AND FUTURE WORK

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.

In future more real time SLP methods can be proposed.

## V. ACKNOWLEDGEMENT

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" published in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 7, JULY 2012.

Also the proposed model is accepted and published by INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH AND TECHNOLOGIES, ISSN: 2278- 0181 (ISO 3297:2007), VOLUME 3 ,ISSUE 2, FEB 2014.

## VI. 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] 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.

[3] 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.

[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] K. Mehta, D. Liu, and M. Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE Transactions on Mobile Computing, vol. 11, No. 2, Feb 2012

[11] Pallavi S.Patil, Prof.J.N.Nandimath, "A Survey Paper on Scalable & Routing Efficient Methods for Source Location Privacy in WSNs", INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH AND TECHNOLOGIES, ISSN: 2278- 0181 (ISO 3297:2007), VOLUME 3 ,ISSUE 2, FEB 2014.