VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ENERGY EFFICIENT APPROACH TO PROTECT SOURCE LOCATION PRIVACY FROM GLOBAL EAVESDROPPER IN SENSOR NETWORK

Karthiga S.
Department of Computer Science and Engineering, College of Engineering, Guindy, Anna University, Chennai, India
E-Mail: karthigaselvaraju@gmail.com

ABSTRACT

Sensor networks are used in monitoring the physical world objects. Generally protocols for sensor network provide secrecy for the content of messages, but contextual information can exposed to adversary. From contextual information, adversary can derive the locations of monitored objects and data sinks. Attacks on these components undermine network applications. Sensor nodes are limited in processing speed and energy supplies. The traditional communication techniques are very expensive to apply for hiding the communication between sensor nodes and sinks. Hence method to provide location privacy that accounts for the resource limitations of sensor nodes is needed. There are number of privacy-preserving routing techniques. Most of the techniques protect against an adversaries which are capable of eavesdropping on a limited portion of the network. Any global eavesdropper can easily eavesdrop on the entire network and defeat these schemes. The recently proposed periodic collection location privacy technique can protect against global eavesdropper. But the drawback is these techniques does not account for energy efficiency which was inevitable as sensor nodes have limited power supply. The proposed energy based routing enhance source location privacy preserving techniques periodic collection method is enhanced as energy efficient to increase the network lifetime.

Keywords: sink, source node, location privacy, adversary, global eavesdropper.

1. INTRODUCTION

A wireless sensor network (WSN) consists of thousands of inexpensive resource constrained miniature devices which are capable of computation, communication and sensing. The WSN mainly rely on broadcasting medium wireless communication which is vulnerable to be eavesdropped. Recent advances in various field of science such as micro electro mechanical systems (MEMS) technology and wireless communications have enabled to develop the low-cost, low-energy consuming, multifunctional sensor nodes that are small in size and communicate in short distances. Sensor network applications require techniques for packet transferring similar to wireless ad-hoc networks. But protocols and algorithms exist for traditional wireless ad hoc networks are not well suited for sensor networks because of its unique features and application requirements.

The unique feature of sensor networks over ad hoc networks is illustrated as below. The sensor network has huge number of nodes than an ad hoc network. Sensor nodes are deployed closely (densely) while ad hoc network nodes are not so. Sensor nodes are prone to failures. The sensor network's topology changes very frequently. Sensor nodes use mostly broadcast communication paradigm whereas most of the ad hoc networks are based on point-to-point communications. Sensor nodes are limited in resource such as power, computational capacities, and memory.

A sensor that detects the signal emitted from source is the source sensor. These source sensors send the information (location) of objects to a data sink (destination) through the intermediate sensors. Monitoring object can be endangered animals in the wild, military soldier, vehicle or robots in a combat zone. An adversary can find the location information of critical components in a sensor network by analysis the traffic pattern of sensors as the packet generation place is probably the source sensor location. Thus an adversary can make use of the communication pattern to locate and then attack the monitored objects. The source location privacy preserving technique against global eavesdropper namely periodic collection is proposed [1].

The routing protocols of sensor network must also contribute to privacy preserving of source and sink locations, which is needed for the primary mechanism of sensor network. Otherwise the adversary can easily attack the objects or base station by exploiting their location. The location of data packet source is hidden by a technique known as source location privacy. The technique also makes an adversary difficult to locate the location of the source. Presently there are protocols which can preserve source location privacy against local adversary which are capable of eavesdrop in limited portion of network. The global eavesdropper can exploit the location information from these protocols. Hence the technique which can preserve location privacy against a global eavesdropper is needed. And the technique must account for energy consumption to increase the network lifetime. There is more energy consumption in nodes near sink than the nodes farther from sink as nodes near sink constantly have to forward data packets from nodes farther from sink .The region with high energy consumption is called as hotspot and nodes in the region die earlier. It leads to creation of energy hole in WSN [8]. The data packets do not reach the sink as nodes around sink are not able to transfer them to sink. It means death of network. Thus network lifetime is specifically depends on energy consumption in hotspots. To increase the network life time there is a need to scatter the energy consumption in hotspot instead of heavy load on a single node. To achieve the balanced energy

consumption the routing based on residual energy is implemented. The residual energy based routing balances the energy consumption among nodes and increases network lifetime. The source location privacy technique periodic collection is enhanced as energy efficient to increase the network lifetime and thus enable them for practical applications.

This paper focuses on energy efficient source location privacy technique in presence of global eavesdropper. The paper enhances periodic collection technique for energy efficient compares them with the existing periodic collection technique to prove that energy efficient techniques are better than previous one. The paper is organized as a section about discussion on existing source location privacy technique, one section on explanation of evaluation parameters used to analyze and compare the techniques, one section on detail description of periodic collection technique and next section is explaining the simulation results of both techniques after that a section to analyze and compare the results, finally a section to conclude the paper and points out the future works.

2. RELATED WORK

In the domain of sensor network, privacy preservation became an active area of research in sensor network. There are two different dimension of privacy threats in sensor network, they are (i) content -based privacy threats and (ii) context-based privacy threats [10]. The content based privacy threats can overcome by cryptographic technique [11]. The cryptographic technique does not address the context-based privacy threats as context-based threats has greater challenges [12]. In the context-based privacy location privacy is important aspect. Particularly there are some techniques for source location privacy to preserve the location of objects. These techniques mainly aim at increasing the safety period. The safety period is defined as the number of messages sent by the source before the monitoring object is successfully located by the attacker [2]. To Provide source location privacy means one has to act against traffic analysis by adversary. The notable solutions for traffic analysis are anonymity, untraceable routes, Unlinkability, unobservable. Anonymity-"Unconditional sender and recipient intractability" provides a stronger and more verifiable version of anonymity as both sender and receiver were made completely anonymous within group [13]. Unlink ability prevent the adversary to relate two things based on a priori knowledge or knowledge gained after a run of the system. Unobservability is a solution which has a set of nodes such as they cannot be observable by any one. Unobservability achieves this by making the communicating nodes as in differentiable from other nodes in the set [12]. The location privacy technique varies depending on the power of the adversary. Based on ability adversaries are differentiated as Local adversaries and Global adversaries. Local adversaries are capable of overhear traffic in only a small portion of the network, typically equivalent to an ordinary node. A local adversary is able to find the source as the packets always follow the same path. Random paths phantom flooding and single-path routing technique are solution to protect against local adversary [14].In the flooding technique [9], the source node send each data packet through numerous paths to a sink, instead of single constant path, thus it makes an adversary difficult to trace the source. In Fake packet generation technique [9], fake sources are created by sink after a sender notifies the base station that it has real data to send. Phantom single-path routing technique [9] achieves location privacy by sending every data packet along a random path before the sink receives it. In Cyclic entrapment [3] looping paths are created at in the network to make the adversary to follow these loops several times and increase the safety period. All the above techniques assume a local eavesdropper as adversary who is capable of eavesdropping on a limited region. But a global eavesdropper can overcome these schemes by locating the first node initiating the communication with the base station, there by locating the source node. There are some recent techniques that consider global eavesdropper as adversary [4], [5].But none of them account for energy conservation.

3. SYSTEM AND EVALUATION MODEL

This section describes about the network model, adversary model and energy model used in simulation and analysis.

A. Network model

In this paper we considered WSN consists of large number of sensor nodes and a sink, which are stationary. Sensor nodes are uniformly deployed in the field and sink in the center of network. The sensor nodes have equal and limited battery power and computation capacity, while sink is provided with unlimited power supply, computation and storage capacity. Sensor nodes communicate each other about their location and energy level to construct their own routing table.

The WSN can be represented as a directed graph G = (V, E, S). The vertices ν V represent the sensor nodes and sink. An edge 〈 u, v〉 ∈ E represents a wireless link between the two nodes u, v V, through which nodes exchange packets.

Objects to be protected have embedded radio frequency (RF) tags and sensor nodes sense the signals emitting from objects and transfer the packet to sink through intermediate nodes. Sink perform two main functions: 1) broadcasting beacon packets to initiate the sensor nodes routing table construction and 2) collecting the data sensed by sensor nodes. Each sensor node can communicate with any other nodes which are within its transmission radius and the communication in the network is bidirectional. The Sink is the sole destination for all the event packets. If sink is within the source sensor node transmission range, the sensor nodes send sensed packet directly to sink or else the source sensor node transmit the packet through multi-hop transmission. Thus sensor nodes communicate each other and with sink. Both the communication is bidirectional.

B. Adversary model

An adversary is a hunter or enemy of monitoring objects. We consider motivated global adversary which can easily eavesdrop over an entire network. Assume that adversary deploy a eavesdropping network with few hundred nodes in the field of sensor network itself to eavesdrop thousands of sensor nodes. Adversary having sufficient energy resource, adequate computation capability and enough memory for data storage and they can continuously eavesdrop traffic for entire sensor network lifetime. An adversary cannot obtain the exact content of the messages intercepted, while the direct sender of the messages can be determined using traffic analysis.

Each adversary node can observe the wireless communication within a certain range and record time, location at which communication occurred as a tuple *(l,t)* where *l* denotes location of observation and *t* is the time at which the particular observation take place.

Adversary nodes communicate their recorded timing and location each other. Thus they can relieve the packet generation location by finding the initial communication and they locate the object easily as the packet generation usually occurs near the object. Adversary is only a passive attacker to eavesdrop the network traffic rather than modifying packets, destroying sensor nodes.

C. Energy model

The Energy model is defined based on energy consumption model. According to this energy model the energy consumption on packet transfer between two nodes depends on distance between transmitter and receiver(d) and number of bits(k) transferring in the packet[7] .

$E_T(k,d) = k\,Eelec + k\,\varepsilon_{fs}\,d^2$, if $d < d0$;
$E_T(k,d) = kEelec + k\,\varepsilon_{amp}\,d^4$, if $d > d0$
$E_R(k) = k\,Eelec$

Transfer energy is denoted by $E_T(k,d)$ and receiver energy is denoted by $E_R(k)$. E_{elec} represents transmitting circuit loss, k is the number of bits in the packet and d is the distance between transmitter and receiver. The model applies for both free space channel and multi-path fading models. ε_{fs},ε_{amp} are energy required for power amplification in free space model and multipath fading model respectively. If distance d is less than threshold d0 ,Power amplifier loss in based on free space model as square of the distance (d2) or else power amplifier loss based on multipath fading as 4th power of distance (d4).

D. Assumptions

Some adversaries can have physical access to sensor nodes and compromise sensor nodes to behave in favor of attacker. But in this paper we assume an adversary does not compromise sensor nodes.

We analysis the source location privacy by assuming that adversary knows the sink location. The set of components whose location needs to be protected (source) is known as Protected set (S_P) and the set of components whose location are known to adversary (sink) is known as Available set (S_A). As already mentioned sinks and sensors are assumed to be stationary while monitored objects can be mobile.

E. Evaluation parameters

To measure how much the particular privacy method is successful in protecting location information of source is given by parameter privacy. The privacy is measure of logical ratio between number of nodes targeted by adversary $|S_T|$ and number of nodes needs to be protected $|S_P|$. It is measured in terms of bits.

Privacy, $b = \log_2 (|S_T|/|S_P|)$

There is a tradeoff between privacy and communication cost. The communication cost is minimum communication overhead needed to achieve the particular privacy level. It is the summation of weight of tree connecting source and sink during each i^{th} event reporting. The Steiner tree is used to calculate the communication cost [6]. Number of events occurred $E= T/(\alpha \times \delta)$.

$$\text{Communication cost } W_T = \sum_{i=1}^{T/(\alpha \times \delta)} Ms\,(i).$$

The optimal privacy is usually achieved with higher communication cost. But lower communication cost is preferable as higher communication cost leads to more energy consumption of nodes which in turn reduces network lifetime. Hence the challenge is achieving optimal privacy without affecting the network lifetime. The proposed energy balanced tree routing achieves the optimal privacy without reducing network lifetime.

The network lifetime is the important parameter to prove the proposed method is energy efficient. The network lifetime is the period from the time network start functioning (S) until any single node loses its full energy and fail to transmit and receive packets.

$$\text{Network life time, } NL = S - \min_{0<n\leq N} (F_n)$$

F_n - failure time of node n.

The latency is the difference in time between when the source detecting the object and sink receiving the event reporting packet. It is measured in seconds. The average latency varies with variation in number of objects.

$$\text{Latency, } L = \left[\sum_{i=1}^{E} (R(i) - D(i))\right] / E$$

Percentage of event detection by sink is the percentage of number of events received by sink out of number of events detected by source nodes. There is tradeoff between event detection rate and privacy achieved

and between number of objects and percentage of events detected.

Event Detection Percentage = RE /DE Where RE is Number of Events received by base station and DE is Number of events detected by source nodes, R(i), D(i) received time and detection time of i^{th} event respectively.

4. PRIVACY PRESERVING TECHNIQUES

The periodic collection preserving technique and its inability to increase network failure is analyzed. Then the steps to enhance periodic collection as energy efficient are explained.

A. Periodic collection

The main aim of periodic collection technique is to protect the location of source from adversaries. The global eavesdropper can find the location of source by finding the area where packet generation takes place as usually packet generation occurs near the object. Thus presences of object determine the traffic pattern. The adversary seriously analyzes the locations where packet generation occurs to exactly locate the source. This technique makes the traffic pattern independent of the presence of objects as every sensor node periodically transmit packets at a particular interval whether there are real data to send or not. Hence the mechanism make the adversary to analyze as much as location as possible by setting every node in the network as target node. Thus adversary has to analyze almost every node behavior to locate objects. This increases the safety period by making adversary to analyze large number. In periodic collection technique optimum privacy is achieved as the number of target node is equal to the total number of sensor nodes in the network.

Privacy, $b = \log_2 |S_T| / |S_P| = \log_2 N / |S_P|$

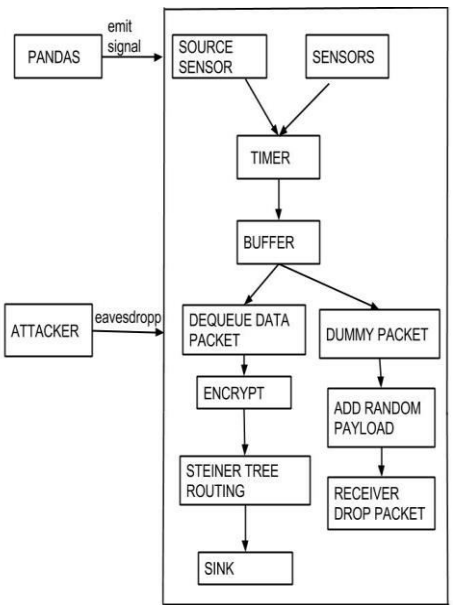

Figure-1. Periodic collection mechanism.

Figure-1 illustrates the mechanism of periodic collection in detail. To implement this technique, each sensor node has a timer which can trigger an event for every particular time interval, for example if the timer interval is set to 20 seconds, every sensor node transmit packet for every 20 seconds. And sensor nodes have a first-in-first-out (FIFO) queue to buffer the received data packets. When the timer fires, the node checks the buffer whether it has any packets in its queue, if it has, dequeues the first packet, encrypts and transmit to the suitable next hop, otherwise, it broadcast a dummy packet with a random payload which will not correctly authenticate at the next hop. Every sensor node only accepts the packets that correctly authenticate.

B. Energy efficient tree routing

The existing periodic collection technique use of simple routing methodology such as base station transmits beacon packets. Sensor nodes construct their routing path on receiving first beacon packets and set the sender as their neighbor. Then the nodes forwards packets to one of its neighbor which is nearest to sink [1].The Periodic collection achieves the optimum privacy, in the cost of high communication cost. Every node in the network has to transmit a packet for every particular time interval. Hence they are drained out of energy quickly. But the mechanism is inevitable to achieve the optimum privacy. To achieve the energy efficiency the energy balanced routing is needed. In the energy balanced routing, the node with highest energy at that time is selected as the next hop. The residual energy of node decreases whenever it transmits the packet. The amount of energy consumption depends on the distance to which it transmit packet. Hence when a node sends packet to a node which is farthest from that, it losses large amount of energy. In the subsequent transmission if the node is again selected as next hop, it drains out of energy quickly. In the existing routing method of periodic collection the node select the next hop which will lead to less number of hop transmissions and hence always selects the neighbor node which is farther to the selecting node. Thus nodes drain out of energy quickly and network lifetime decreases.

In the proposed energy efficient routing, routing table has additional field residual energy of neighbor along with their hop count and distance. As nodes are stationary, hop count and distance are same throughout the network life hence nodes send their hop count and distance information only once during the initial routing table construction. The energy of nodes decreases for computation work and in greater rate while communication with other nodes. The residual energy of nodes varies for nodes with times according to their number of communication. So, energy efficient routing allows nodes to frequently update the residual energy of neighbors. Thus the sensor nodes aware about the present residual energy of neighbors.

When transmitting and receiving the data packets, node is selected as next hop by considering hop count and residual energy. For example when a node first time selected as next hop the residual energy obviously higher

and due to that transmission energy decreases. Then for second time when the same node is considered for next hop, its energy level in routing will be lower than other possible next hop. So another neighbor having the same or next lower hop count of previous next hop with higher energy is selected as next hop for that particular routing. Then the routing also compare the residual energy of nodes and the energy needed to transmit the packets and decide whether the node is able to transmit the packet before drain energy. As a whole, node failure due to power loss will be reduced, energy between the nodes is balanced over nodes thus network failure due to more energy consumption in only few nodes is avoided, in turn it increases the network lifetime considerably.

5. SIMULATION EVALUATION

In this section the simulation of periodic collection and energy efficient periodic collection is illustrated separately. In both simulations, a sensor network is deployed with equal number of objects. Each object has an electronic tag that emits a signal that can be detected by the sensors in the network. The sensor network consists of 5,093 sensor nodes and they are distributed randomly in a square field of 1000 x 1000 square meters to monitor the pandas. The base station is the destination for all real data packets and it is located at the center of field (500, 500). Figure-2 shows the rough layout of sensor network field used in simulation. Each sensor node can transmit data packets to other sensor nodes in a radius of 50 meters, and they can detect signals emitted by objects within 25 meters. Each sensor node has average of 40 neighbors and that the presence of any object will be detected by 10 sensor nodes. Assume an application that needs to report only the location of object to base station.

We deploy the adversary network in the same field of sensor network in the grid manner with 100 nodes to simulate the global eavesdropper. Each adversary nodes can eavesdrop the sensor network traffic within a range greater than the transmission radius of sensor node and observe the time and location pair (t, l) of packet transmission. The adversary nodes communicate observed information to the neighbor adversary node and can deduce the packet generation location. The packet generation location is nearer to the object; hence the adversary can approximately locate the source (object).The simulation shows that proposed location privacy technique resist against the global eavesdropper.

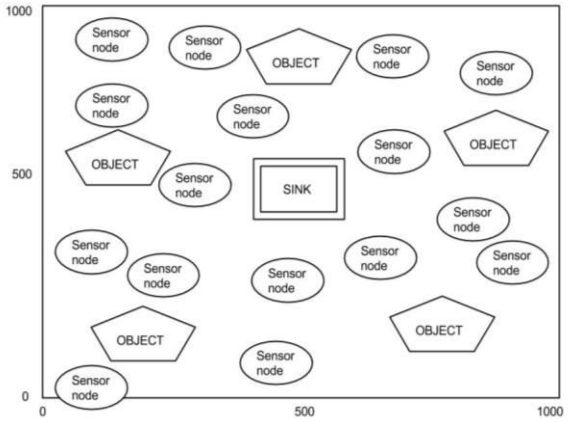

Figure-2. Network field layout.

Both periodic collection methods are simulated with communication interval of 20 seconds and buffer size is fixed as 20. For energy efficient periodic collection 500 nodes are included but they won't sense object as source sensor. They won't sense objects and used only for forwarding of packets. The simulation is done for 5, 10, 20, 40, 80 number of objects. Each simulation is run for 1000 intervals. The latency, privacy, communication cost, network lifetime and percentage of event detection by sink are measured for each simulation. The evaluation parameters values of periodic collection and enhanced periodic collection are compared.

6. COMPARISON

The periodic collection and energy efficient periodic collection is compared by the values obtained for latency, privacy achieved, communication cost required and percentage of event detected by sink. As simulation done by varying number of objects, the evaluation parameters values are also compared with respect to number of objects for both the methods to conclude which method is suitable for practical application with larger number of objects to be protected. Latency, event detection, percentage, communication cost are better for energy efficient periodic collection than existing periodic collection. More importantly the network lifetime increases for energy periodic collection enhanced with energy efficient routing.

Table-1 shows that the latency of energy efficient periodic collection is constantly lower than the latency of periodic collection technique for any number of objects. And it shows that, for both the method the privacy decreases with increasing number of sources. As the number of sources increases, the target set contains more number of protected sensors, it leads to fall in the ratio between N and SP. But in each case, the privacy is considerably higher than the privacy of periodic collection. Then it illustrate that the percentage of event detection by sink is higher for energy efficient periodic collection method even for larger number of objects. Then the variation of privacy with respect to different number of source is compared target set contains more number of protected sensors, it leads to all in the ratio between N and

SP. Finally it shows the network lifetime of both periodic collection and energy efficient periodic collection method with different numbers of objects. From the table it is clear that the energy efficient periodic collection increases the network lifetime in greater extend. The communication cost is constant for any number of objects as every node transmits packets periodically. As number of object is higher in efficient periodic collection, communication cost is higher but it does not affect network lifetime. The similar variation is pictorially shown by following figures (Figure-3 and Figure-4).

Table-1. Simulation results.

No. of objects	Periodic collection	Energy efficient periodic collection
	latency (Intervals)	
5	14.21	11.94
10	16.81	12.79
20	17.04	13.91
40	18.09	17.10
80	18.86	18.05
	Privacy (BITS)	
5	6.613	6.850
10	5.699	5.96
20	4.620	4.857
40	4.090	4.326
80	3.917	4.288
	Percentage of event detection %	
5	100	100
10	94.89	100
20	83.57	94.68
40	61.20	85.28
80	58.45	77.85
	Communication cost	
5,10,20,40,80	41684	51106
	Network life time (Intervals)	
5	>1000	>1000
10	410	>1000
20	300	>1000
40	100	710
80	50	520

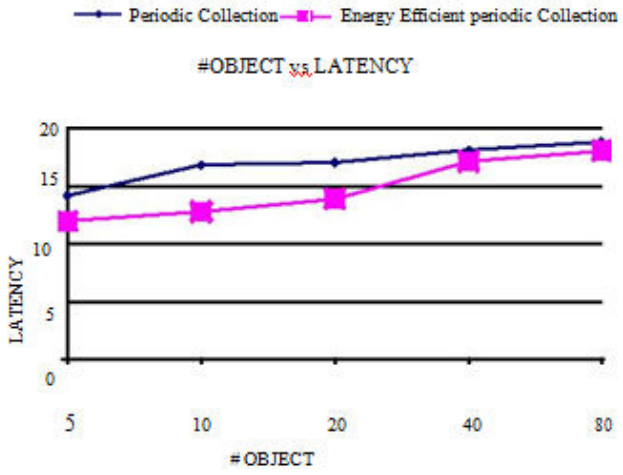

Figure-3. Object Vs latency.

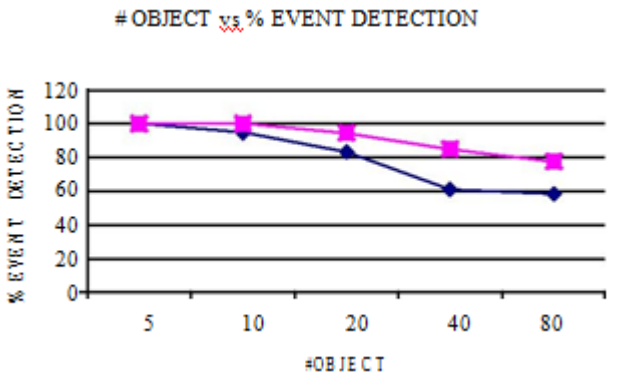

Figure-4. Object Vs event detection percentage.

7. CONCLUSIONS

The comparison shows that energy efficient periodic collection is better than the periodic collection in terms of latency reduction, increasing packet delivery ratio and increasing network lifetime. As the energy efficient method uses the energy based routing, probability of node failure is reduced and although any node fails, its neighbor have the knowledge about its energy level hence they transmit the data packet through alternate path. But in periodic collection nodes continuously transmit data packet to failure nodes as they don't have knowledge about and the disabled nodes can't transmit the packets. So, the packet delivery ratio is much lesser in periodic collection method than the energy efficient periodic collection. And we can notice that the first node failure time is much longer for energy efficient technique as they try to balance the energy between nodes. In the energy efficient method node fail only when there is no other neighbor with higher energy is available, as node with lower energy has to transmit the packets. It depicts that energy efficient periodic collection increases the network lifetime along with the optimum privacy is achieved. As; future work, I am working to enhance source simulation location privacy technique. Sometime the sensor nodes can be compromised by attacker to obtain critical information easily. In this work I assumed that sensor nodes are not compromised. Source location privacy under compromised attack can be enhanced as energy efficient in future.

REFERENCES

[1] Kiran Mehta, Donggang Liu, Member, IEEE, and Matthew Wright, Member, IEEE "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", IEEE Transaction On Mobile Computing,Vol. 11, No. 2, pp.320-336, February 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] Y. 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.

[4] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.

[5] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008.

[6] H. Takahashi and A.Matsuyama, Math. Japonica "An Approximate Solution for the Steiner Problem in Graphs," vol. 24, No.6, pp. 573-577,1980.

[7] Sourabh Jain, Praveen Kaushik, JyotiSinghai "Energy Efficient Maximum Lifetime Routing For Wireless Sensor Network", International Journal Of Advanced Smart Sensor Network Systems, Vol 2, No.1,pp.1-11, January 2012.

[8] A.-F, Liu, P.-H. Zhang, and Z.-G. Chen, ''Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks,'' J. Parallel Distrib. Comput., vol. 71, no. 10, pp. 1327–1355, 2011.

[9] 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

[10] A. Jhumka, M. Leeke, and S. Shrestha, ''on the use of fake sources for source location privacy: Trade-offs between energy and privacy,'' Comput. J. vol. 54, no. 6, pp. 860-874, 2011.

[11] L. Lamport, R. Shostak, and M. Pease, ‘‘The Byzantine generals problem,’’ ACM Trans. Program. Lang, Syst. vol. 4, no. 3, pp. 382-401, 1982.

[12] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, ‘‘SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealthsystems, ’’IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 365-378, May 2009.

[13] M. Conti, J. Willemsen, and B. Crispo, “Providing Source Location Privacy in Wireless Sensor Networks: A Survey,” pp. 1- 43, 2013.

[14] R. Rios and J. Lopez, “Analysis of location privacy solutions in wireless sensor networks,” IET Commun. vol.5, no. 17, p. 2518, 2011.