ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

Maximizing Lifetime through Phantom Node for Privacy Preservation in WSN

[1] A.O.Shini [2] Dr. Satish Devane,
[1] Computer Department, [2] Computer Department
[1][2]Datta Meghe College of Engineering
Mumbai, India
[1] mrsshinisaji@gmail.com[2] srdevane@yahoo.com

Abstract: **One of the major challenges in real-time event-monitoring applications such as military surveillance or monitoring of endangered species of Wireless Sensor Network (WSN), is that of context privacy in terms of location of source node. When a source node senses and forwards a packet to the target, adversaries can eavesdrop on network and trace source node from base station. The concept of introducing phantom node is to act as intermediate nodes between actual sources and sink, so that the privacy of source node is preserved. Phantom nodes can thus help in achieving privacy. But while trying to achieve this, it is also essential to ensure that the lifetime of sensors are not affected due to resource constraints in the sensor nodes. This paper attempts to use an energy efficient algorithm for establishing phantom node so as to improve network lifetime of sensors while achieving source location privacy.**

***Keywords*— WSN, energy efficient algorithms, privacy**

I. INTRODUCTION

Wireless sensor network (WSN) that monitors an asset, it is important to safeguard the sensors that sense the target from adversaries who eavesdrop on network. The privacy of source sensor node location is vital as adversaries try to locate it through routing patterns. Protection of source sensor node is achieved by introducing phantom node to distract the attention of adversary from the real source. An adversary can trace back from base station towards the real source node by traffic backtracking attack but ultimately can never reach real source node as they can only trace back up to the phantom node.

Many researchers have used complex algorithms to establish phantom node has an impact on the network lifetime of sensors. Hence the method of establishing it should be energy-efficient. The location of the phantom node from the sink is equally important. A phantom node should not be too close to the sink as it will not help against adversaries monitoring the entire network. Also, if the phantom node is too far from the sink then the energy consumed is more in the network because of the lengthy routing paths. Hence phantom nodes are selected in such a way so as to achieve source node privacy without compromising on the lifetime of sensors.

This paper we have used an energy-efficient algorithm to establish phantom node, after establishment of phantom node, the message packet is forwarded to the base station via a backbone network that routes the packet to the sink. Diversionary routes are created on the backbone nodes so that the adversary finds It Difficult To Back Trace To The Phantom node and thereby the source location node. Dummy messages are transmitted in the network in order to safeguard the network from global eavesdropping.

II. WIRELESS SENSOR NETWORK

Wireless sensor networks (WSN) finds its way where real time event sensing and monitoring is necessary. Sensor networks have been widely employed in many monitoring-based applications such as gathering data in applications such as highway traffic, battle field reconnaissance, and habitat monitoring of endangered animal species. A WSN comprises of numerous wireless sensors that communicate among themselves wirelessly in an open environment. The constraint most often associated with sensor network design is that sensor nodes operate with

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

limited energy budgets. Typically, they are powered through batteries, which must be either replaced or recharged (e.g., using solar power) when depleted [1]. So it is essential to maximize the lifetime of the network.

A. Privacy issues in WSN

One of most obvious challenges appearing to threaten the successful deployment of sensor networks is the concern of privacy issues. Sensor networks normally consist of a set of low-cost radio devices that operate on readily-available, standardized wireless communication technologies. Therefore, the open-architecture of underlying sensor technology results in a privacy breach due to the following reasons:

- Adversaries can eavesdrop wireless signals transmitted between sensor nodes
- Sensors are vulnerable to people as they can access it physically in an open environment.

There are two types of privacy concerns: data oriented and context oriented. Data-oriented concerns deal with privacy of data collected from a WSN or queries posted to a WSN by peers. There are various encryption techniques to protect the confidentiality of the message content. Context-oriented concerns focuses on contextual information such as location and timing of traffic flows in a WSN.

There can be two types of attacks for exploiting privacy: local [2]-[4] and global [5]-[7] eavesdropping. Local eavesdropping involves listening to wireless communication signals and tracing back from base station to source node. While doing so, the transmitted packet data may not even be analyzed. This traffic backtracking attack can be prevented by phantom routing [8]. This protocol aims at selecting a phantom source node at a location far away from the real one (camouflage step) and then routing the packet towards the base station through flooding, probabilistic broadcast or single path routing. In order to be effective against a global adversary, dummy packets have to be introduced and propagated in the network even if actual data packets are not transmitted.

III. RELATED WORKS

In the past decades, a number of communication protocols have been proposed for achieving source-location privacy. One of the major challenges in trying to achieve privacy is to assure that the network lifetime is not deteriorated. Much research is done in this area. Ref. [21] proposes ant colony optimization (aco) that provides an intrinsic yet natural way of exploring the search space so as to preserve the sensor's location privacy based on the pheromone value on its link and the two parameters pheromone trail and heuristic value. The more the energy level of the sensor node, the better is the probability of the node getting selected for the next hop. This energy efficient source location privacy protecting scheme (eelp) prevents the adversary from back tracing to the source node. Though this approach is energy efficient, the adversary still has the probability to find the source node by monitoring and analyzing the message routing paths. In other words, the scheme may achieve privacy preservation against a local eavesdropper but may not effectively work against a global eavesdropper. Hence context privacy is not achieved to its fullest extent.

An energy-efficient cyclic diversionary routing (cdr) scheme against global eavesdroppers is proposed in [11] to safeguard contextual information. The entire network is divided into several rings in the non-hotspot areas which are further divided into clusters each having a cluster head. In each period, the ring where the object appears must establish cyclic diversionary route. Network security in terms of privacy is achieved due to the generation of dummy packets in the network rings synchronous to the real event message generation. Lifetime is not deteriorated due to the dummy message generation as the cluster heads act as filters and dump dummy packets. Only real packets are forwarded to the promoter and thereby to the sink. Also, the rings in the non-hotspot regions have diversionary routes established. Hence there is no deterioration in the network lifetime.

In [20], to preserve privacy and increase network lifetime, fake sources and fake source areas are created in the non-hotspot regions where the energy is abundant. Fake sources are nodes selected randomly and holding a token. Though the increase in fake source areas can lead to better levels of privacy, the network lifetime can be affected due to the increase in the communication overhead between the nodes.

A technique known as sink toroidal region (star) routing [13] is proposed in order to provide source-location privacy with low energy consumption. The source node

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

randomly selects an intermediate node within a particular area located around the sink node. The selection of the intermediate node and all message packets routed through it instead of the source directly leads to source location privacy. Energy consumption is low as the intermediate node is selected from a non-hotspot region. Though privacy can be achieved to some extent, there is no mechanism to safeguard against a global eavesdropper that monitors the entire network.

A tree-based diversionary routing scheme [12] is proposed for preserving source location privacy. Diversionary routes are created from the nodes on the backbone route and also dummy packets are generated in the network to prevent global eavesdropping. Though this routing protocol achieves significant improvement in lifetime, the establishment of phantom node is in such a way that it is only far away from source. The distance of phantom node from the sink is not considered. Hence there should be a better method of establishing the phantom node.

Much research has been done on achieving contextual privacy in terms of source location. Most of the work focuses on achieving this by compromising the network lifetime factor. Some papers focus only on local eavesdropping without safeguarding against global eavesdropping. The usage of sensors lying in non-hotspot areas contributes to lesser energy consumption. Many algorithms that aim to achieve privacy as well as network lifetime has been least tolerant to delay and hence can be used only for latency-tolerant applications.

IV. PROPOSED SOLUTION

One major challenge that is posed in asset monitoring applications on wireless sensor networks (WSN) is to provide confidentiality to the source sensor's location against an adversary who is trying to gain access to the asset. The adversary might accomplish this by capturing wireless signals through low-cost sensor devices running in a monitor mode or through sophisticated software radios capable of monitoring a broad array of radio technologies. Most of the previous work that has attempted to achieve source location privacy has compromised the network lifetime factor. This is also true the other way round. Some research that has been done to improve lifetime has fallen short of privacy. Complicated algorithms may help in achieving source location privacy but most of the time comes at a cost of increased energy consumption by the resource-constrained sensors. Thus lifetime in WSN is affected. Hence, it is important to improve network lifetime while also preserving the source location from adversary. Our proposed system can achieve improvement in network lifetime without affecting the source location privacy.

The adversaries in a wireless sensor network are continuously trying to capture target or an asset by sensing the source location. To achieve this, they reverse hop from base station or from any other node inside the network. In order to safeguard the source sensor node from being tracked by adversaries, a system should be implemented in such a manner that the energy consumption of resource-constrained sensors is reduced. This is achieved by establishing energy-efficient phantom nodes.

A. Implementation

In our proposed system, we attempt to improve network lifetime of sensors through establishment of energy efficient phantom node in tree-based diversionary routing while preserving privacy against eavesdropping. Much of our work will be based on [12].

First, a source node which is guarding an asset randomly picks and forwards message packets to the phantom node, say p which lies in the non-hotspot region. Hence p is established in what we propose as the chillspot region. The hotspot region is the circular region around the sink with a maximum radius, say r. The sensors in the WSN are spread across a geographical area around the sink with a maximum radius, say r. The non-hotspot region area is an area within the wireless sensor network with at least a minimum radius distance, r, from the sink node and a maximum distance r away from the sink node. Hence the phantom node should have radius r_p, such that $r<r_p<r$ so as to limit the energy consumption in the routing path.
To optimize the energy consumption, we establish the phantom nodes so as to meet the following criteria:

- Phantom nodes should be located far away from source node.
- They should not be placed too far or too close from the sink node.
- Every intermediate node or phantom node should have equal probability of being selected randomly.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

- A backbone route is established with nodes that reach the sink and each node has diversionary routes on its branches. Phantom node should be a node in the branch route of a backbone node.
- Phantom nodes cannot be a node on the backbone route in tree-based diversionary routing scheme so as to help achieve privacy.

If x_0, y_0 are the coordinates of the sink node location, the source node randomly selects a location (X,Y) so that

$$(X,Y)=(X_0+DCOS(\Theta),Y_0+DSIN(\Theta)) \quad [13]$$

Where d is selected uniformly from [R,R]

And θ is selected uniformly from $[0,2\pi]$

Once the packet is forwarded to this location called the chill spot, it is then routed to the header node of the containing grid. In case there is no node at that location, the last node in the routing path becomes the phantom node and in turn routes the packet to its own grid's header node. Every node in this area has equal probability of being selected as the phantom node.

B. Algorithm description

Fig. 1 shows a wireless sensor network with labelled nodes as active and all other nodes as inactive.
Node s is the source sensor node and senses a target and prepares a packet to be sent to the base station bs. S establishes a phantom node p which lies in the chillspot region and forwards the packet to p.
P routes the packet to the intermediate node a on the backbone route to the base station bs. P also initiates dummy packet request to a node farther from the sink and receives it and the process continues until network border is reached.

The intermediate node a forwards real data packets to the base station bs through all the intermediate nodes. Also a sends dummy packet requests to node farther from the sink and receives from it. This process also continues until network border is reached. Nodes b, c, d, e and f are involved in sending and receiving dummy packets. Every node that receives the dummy packet request also creates a diversionary route requesting and receiving dummy packets until network border is reached. The intermediate node d creates a diversionary route through nodes u, v and w.

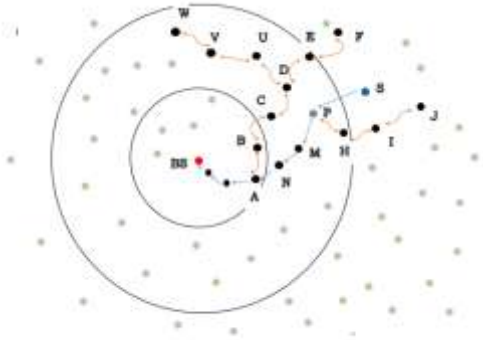

Fig 1 Routing Packets From Source To Sink Through Phantom Node

V. RESULTS & ANALYSIS

As we have stated in our problem definition, the main aim is to improve the lifetime of WSN. While trying to do so, the source location privacy is also preserved. As our work is majorly based on ref. [12], efforts have not been made to further improve privacy. Privacy of source node is preserved as we continue to create diversionary routes on backbone route nodes towards network border farther away from the sink. Thus high privacy is attained as the adversary on reverse tracing comes across two branches every time and hence probability of choosing the right path is only 0.5.
Ref [12] already states that diversionary routes are created on nodes lying in non-hotspot region and hence by using these nodes with abundant energy, the lifetime is improved. In addition to this, our proposed system calculates how far the phantom node should appear from sink. The nodes near to sink consumes more energy as they are involved in data aggregation. If phantom node is positioned near the sink, the tracing of adversary becomes easier. If the phantom node is far away from the sink, then the routing will affect the lifetime of the network. Hence our implementation chooses a chillspot to further improve lifetime.

A. Range VS lifetime:

In a wireless sensor network, if the distance between two nodes is less than or equal to the transmission range, then they are said to be connected. Otherwise, if the distance between them is more than the transmission range, they are unable to send or receive packets and are disconnected. Sensors in a wireless sensor network spend more energy in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

data communication over other aspects like sensing, computation and data aggregation. Fig. 2 shows the simulation results for lifetime with respect to varying ranges in the form of xgraph generated in ns2.

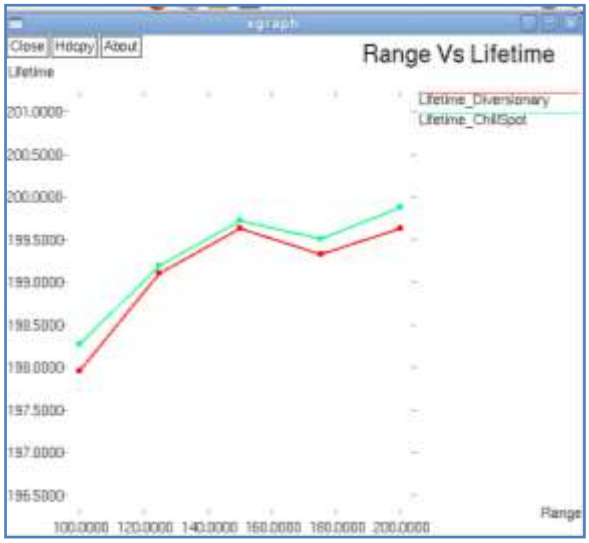

Fig 2 Xgraph of Range Vs Lifetime

In our proposed system, the lifetime with respect to the transmission range is improved over the existing system. Table 1 tabulates the lifetime values under varying range values with respect to the X graph generated.

Table I Range VS Lifetime

Range	100	125	150	175	200
Lifetime in Diversionary routing	197.963	199.109	199.63	199.329	199.626
Lifetime in Chill Spot	198.27	199.19	199.718	199.506	199.881

Range VS hop count

In wireless sensor networks, the number of hops between the source and the sink has a significant impact on network performance. At an optimal range value between the sensor nodes, the hop count decreases, and hence there will be lesser average delay. But when the range further increases from the optimum value, the lifetime of these nodes reduces as more transmit power is required. In our proposed system, when the range increases the hop counts involved are more when compared to the existing system. Hence there is more delay in the packet reaching the destination.

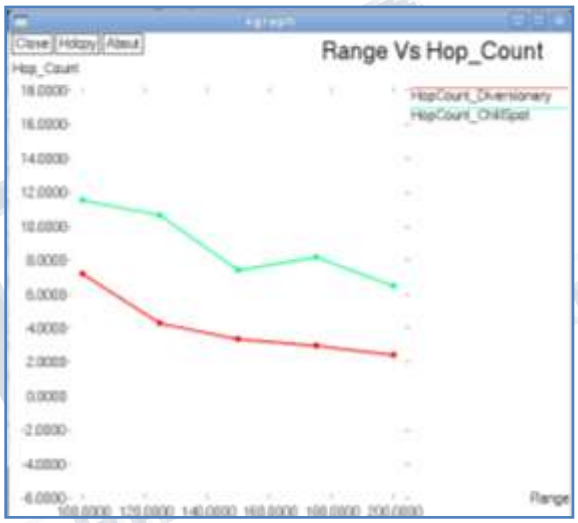

Fig 3 Xgraph Of Range Vs Hopcount

Other findings:

In addition to lifetime improvement, our system also improves packet delivery ratio, message latency, jitter and throughput.

VI. CONCLUSION

With the increase in pervasive computing, source location privacy preservation has become more important. Our work has focused in establishing energy efficient phantom nodes so that it is neither far nor near to the sink

node. This has led to privacy preservation as well as lifetime maximization. Also dummy message generation in the network prevents global eavesdropping by the adversaries. The establishment of tree routes from the backbone nodes away from the sink towards the network border has led in increase of safety period and trace time by the adversary. The privacy of source location has been achieved by utilizing the residual energy of sensor nodes in remote regions and thereby reducing the energy consumption of nodes near to the sink.

REFERENCES

[1] Genita gautam, biswaraj sen, department of computer sc & engineering sikkim manipal institute of technology, sikkim manipal university,sikkim, design and simulation of wireless sensor network in ns2, international journal of computer applications (0975 – 8887) volume 113 – no. 16, march 2015

[2] C. Ozturk, y. Zhang, and w. Trappe, ``source-location privacy in energy-constrained sensor network routing," in proc. 2nd acmworkshop securityad hoc sensor netw. (sasn), vol. 4. 2004, pp. 88_93.

[3] Y. Li and j. Ren, ``preserving source-location privacy in wireless sensor networks," in proc. 6th annu. Ieee commun. Soc. Conf. Sens. Mesh adhoc commun. Netw., jun. 2009, pp. 1_9.

[4] H.wang, b. Sheng, and q. Li, ``privacy-aware routing in sensor networks," comput. Netw., vol. 53, no. 9, pp. 1512_1529, 2009.

[5] K. Bicakci, h. Gultekin, b. Tavli, and i. E. Bagci, ``maximizing lifetime of event-unobservable wireless sensor networks," comput. Standards interf.,vol. 33, no. 4, pp. 401_410, 2011.

[6] K. Bicakci, i. E. Bagci, and b. Tavli, ``lifetime bounds of wireless sensor networks preserving perfect sink unobservability," ieee commun. Lett., vol. 15, no. 2, pp. 205_207, feb. 2011.

[7] M. Shao, y. Yang, s. Zhu, and g. Cao, ``towards statistically strong source anonymity for sensor networks," in proc. 27th conf. Comput. Commun.ieee infocom, phoenix, az, usa, apr. 2008, pp. 51_55.

[8] Pandurangkamat, yanyong zhang, wade trappe, celalozturk,"enhancing source-location privacy in sensor network routing", proceedings of the 25th ieee international conference on distributed computing systems(icscs'05), 2005

[9] http://www.tutorialsweb.com/ns2/ns2-1.htm

[10] f. Shebli, i. Dayoub and j.m. Rouvaen, "minimizing energy consumption within wireless sensors networks", university of valenciennes (iemn, umr cnrs 8520)

[11] Ju ren, yaoxue zhang, kang liu, "an energy-efficient cyclic diversionary routing strategy against global eavesdroppers in wireless sensor networks"

[12] Jun long, mianxiong dong, kaoru ota, anfeng liu, "achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks", ieee 2014

[13] Leron lightfoot, yun li, jian ren, "preserving source-location privacy in wireless sensor network using star routing", ©2010 ieee

[14] Sajalk.das, bhavanithuraisingham, na li, nan zhang "privacy preservation in wireless sensor networks :a state of the art survey, adhocnetworks 7(2009) 1501-1514

[15] G. Tan,w. Li, and j. Song, ``enhancing source location privacy in energy-constrained wireless sensor networks," in proc. Int. Conf. Comput. Sci. Inf.technol., 2014, pp. 279_289.

[16] K.mehta, d. Liu, and m. Wright, ``location privacy in sensor networks against a global eavesdropper," in proc.

Ieee int. Conf. Netw. Protocols (icnp), oct. 2007, pp. 314_323.

[17] H. Chen and w. Lou. (2014),"on protecting end-to-end location privacy against local eavesdropper in wireless sensor networks", pervas.mobilecomput.[online].

[18] A. Jhumka, m. Bradbury, and m. Leeke,"fake source-based source location privacy in wireless sensor networks",concurrencycomput.,pract.experience[online]. available: http://onlinelibrary.wiley.com/doi/10.1002/cpe.3242/pdf

[19] http://ns2blogger.blogspot.in/p/n.html

[20] Zhiwen zeng, xiaoyan hu, zhigang chen,"preserving source-location privacy in wireless sensor networks against a global eavesdropper", int'l conf. Wireless networks | icwn'15

[21] Xin wu, yufei xu, da teng, "an improved method based on self-adjusting directed random walk approach for preserving source-location privacy in wireless sensor network"