Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 5, May -2015

Achieving Source Location Privacy in WSNs by using Multiple k-hop Clusters based routing technique

Pooja K Akulwar [1], Prof. Disha Deotale[2]

[1] Department of Computer Engineering, GHRIET, Pune, poojaakulwar13@gmail.com
2 Department of Computer Engineering, GHRIET, Pune, dishadeotale@raisoni.net

Abstract — *In recent years, source location privacy has become significant challenge in Wireless sensor networks. Source location privacy is to hide the physical location of the actual source and makes it more complex for an adversary to trace back the path to the source location. Radio frequency Localization Techniques can be used by adversaries so that they can trace reverse path hop-by-hop from sink to source and identify the source. Many privacy related techniques such as Phantom routing, cloud based routing, Tree based diversionary routing etc have been established, but still there exits some problem in terms of source location privacy. Hence, to preserve source location privacy and to maintain energy efficiency, Multiple k-hop clusters based routing strategy (MHCR) can be used. In this scheme, various interference clusters are formed in entire network. Each sensor in cluster acts as a Fake source. Due to this adversaries get confused and unable to trace the reverse path towards source. Also cluster heads are used to filter dummy traffic formed by Fake sources so that there is no rise in energy consumption in hotspot of network. MHCR provides energy efficiency without reducing network Lifetime and preserves source location privacy in Wireless Sensor Networks.*

Keywords- Wireless Sensor Network, Multiple k-hop Clusters based routing, Cluster heads, Network Lifetime, Energy efficiency.

I. INTRODUCTION

Wireless sensor network (WSN) 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. A sensor network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Sensor networks have a variety of applications such as environmental monitoring, condition based maintenance, habitat monitoring, seismic detection, military surveillance, inventory tracking, smart spaces etc.

A Wireless sensor network is vulnerable to threats and risks. The major issue that needs to be addressed is privacy of source node. Source location privacy is to hide the physical location of the actual source and makes it more complex for an adversary to trace back the path to the source location.

To address source location privacy for wireless sensor networks multiple privacy techniques have been researched. One of the techniques called phantom routing exist which provide efficient and private sensor communications and is capable of protecting the source's location. Phantom routing approach preserves the actual data packets along with the source location. In this routing approach, source sends data to the phantom node which acts as a decoy & then forwards that data to sink node by using the shortest path. But this scheme has phantom node which is routed to sink directly. Hence, adversaries can trace the reverse path along the route of Phantom node and reach the source. As lots of Phantom nodes are created, energy consumption of sensor nodes increases. Since energy consumption in phantom routing increases, Network Life time decreases.

Routing-based schemes try to preserve source location privacy by sending packets through different routes instead of single route. This increases complexity for adversaries to trace back packets from the Sink to the source node because they cannot receive a continuous flow of packets. However, if the adversary has larger overhearing range than the sensor nodes' transmission range, then there are chances of capturing a large ratio of the packets sent from a source node [2].
If pandas remain present in one location for more time, an adversary can capture lots of packets though that packets are transmitted through different routes.

It is a very challenging task to provide source-location privacy under the global adversary model. To prevent the traffic analysis attacks and security metrics such as privacy and network lifetime widely exist. If all the packets in the network are real event packets and every node reports, receives, or forwards a real event message immediately, it would be quite easy for a global attacker to trace back to the real source without any delay.

Therefore, diversionary routing paths came into existence in the sensor network in which multiple routes are present so that adversaries get confused and face difficulty in reaching the source node. Multiple fake nodes are generated at the end of each diversionary route. The source node and the fake node both have same size so that adversaries cannot differentiate between original and fake data packet. As there are lots of fake nodes, extra energy consumption occurs which lessens the network lifetime.

To hide the presence of events from adversaries with a global hearing range, in [3] all sensors transmit messages at a fixed rate regardless of the existence of real events. This provides privacy but the cost is unacceptable for battery-powered devices. The number of clustering algorithms has been proposed to improve the lifetime of the sensor network.

But all these privacy techniques utilized in general network scenarios are not appropriate for protecting the source location in a sensor network. Many methods causes overhead in the network, some leads to increase in packet collision, some decreases network lifetime. One of the ideas to preserve source location privacy is to use multiple k hop clusters based routing technique which will provides source location privacy and proves efficient in energy consumption without decrease of network lifetime. The rest of the paper is organized as follows: section-2 describes the related work and the section-3 concentrates on source location privacy preserving technique- multiple k-hop clusters based routing technique in detail.

II. RELATED WORK

1. Multiple k-hop clusters based routing scheme to preserve source-location privacy in WSNs

Ren , Zhang Yao-Xue, Liu Kang[1] has proposed a multiple k-hop clusters based routing strategy (MHCR) in which various interference clusters are formed in entire network. Each sensor in cluster acts as a Fake source. Due to this adversaries get confused and unable to trace the reverse path towards source. Also cluster heads are used to filter dummy traffic formed by Fake sources so that there is no rise in energy consumption in hotspot of network.

The authors through their analysis stated that MHCR provides energy efficiency without reducing network Lifetime and preserves source location privacy in Wireless Sensor Networks. They have done systematic security analysis on protecting tracing back attacks and stated that purpose of routing is to deliver messages to sink and enhance location privacy & energy efficiency without decreasing network lifetime. MHCR improves security by creating interference clusters.

2. Enhancing Source-Location Privacy in Sensor Network Routing

To achieve source location privacy, the authors Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk [2] proposed a phantom routing technique that enhance privacy protection.

The authors stated that in phantom routing the source node send data to the node called phantom node which acts as a decoy & forwards that data to the sink. The goal here is to keep the adversary away from the source node. As a result, a privacy routing technique should prevent adversary from locating the location of source while delivering data to the sink.

3. Location privacy in sensor networks against a global eavesdropper

Mehta K, Liu D, Wright M.[3] have formalize the location privacy issues under the model of a global eavesdropper and shown the minimum average communication overhead needed for achieving a given level of privacy. They presented two techniques to provide privacy against a global eavesdropper- a periodic collection method and a source simulation method.

The periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides trade-offs between privacy, communication cost and latency by imitating the behavior of real objects at several places in order to confuse adversaries.

4. Source-Location Privacy in Energy-Constrained Sensor Network Routing

Celal Ozturk, Yanyong Zhang, Wade Trappe[4] focused on protecting the source location by introducing appropriate modifications to sensor routing protocols to make it difficult for an adversary to backtrack to the origin of the sensor communication. In particular, they focused on the class of flooding protocols. They observed that in Flooding technique source node send each packet through various paths to sink. Hence the adversaries face difficulty in tracing path. But the sink receives the real data packet from source through shortest path. Therefore, adversaries can identify that path and trace source node. This method consumes large amount of energy than others.

By observing prior method, authors have proposed flexible routing strategy, known as phantom routing. Phantom routing is a two-stage routing scheme that first consists of a directed walk along a random direction, followed by routing from the phantom source to the sink. This routing technique is capable of keeping the adversary virtually lost within the network. This is the hop based approach in which phantom node is kept away from source node so that it is difficult to identify source node location. But this method causes lots of energy consumption.

5. Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks

Yun Li and Jian Ren [5]proposed two-phase dynamic routing stragies for preserving source location privacy. In this strategy, the message is transmitted to sensor node which is located far away from sensor node and that message is transmitted to sink. The authors first described routing through a single randomly selected intermediate node away from the source node. Later the authors presented routing through multiple randomly selected intermediate nodes based on angle and quadrant to further improve the global source location privacy.

III. SOURCE LOCATION PRIVACY PRESERVING TECHNIQUE

For preserving source location privacy, one of the best solutions is to use multiple k-hop clusters based routing technique. The principles of Multiple k-hop clusters based routing scheme are:-

1. All interference k-hop clusters and routing path are homogeneous.
   As they are homogeneous, adversaries cannot differentiate between them and hence get confused.
2. Network Lifetime depends on energy consumption in the hotspot.
   Network Lifetime is inversely proportional to energy consumption. To increase Network Lifetime, dummy traffic in the hotspot must not allow so that energy consumption does not increase. Even energy consumption in other areas should be controlled in such a way that it must not be greater than hotspot region.
3. Energy is required to create interference clusters.
   To improve energy efficiency, abundant energy in outer regions of network is utilized in creating as many interference clusters as possible.

3.1 Overview of Multiple k-hop clusters based routing scheme

Based upon the hop counts between source and sink, the network is divided into several rings. Multiple k-hop clusters are created in the same ring.

- The cluster consists of k-hop. Real source walks randomly 'p' hops to select the origin of interference cluster head (ICH). This ICH is selected before data is delivered to sink. The ring in which ICH is present is called Interference ring (IR). Then origin ICH launches circular routing to allocate remaining ∂-1 ICHs in particular IR. Later each of ICH starts to cluster with k hops.
- When the clusters are formed, intra cluster data aggregation is conducted by ICH. This data aggregation is conducted within the members of particular ICH. TDMA hop by hop method is used for this.
- The intra cluster communication consists of communication in which all sensors stores only real data that is generated by real source. This real data is forwarded in their time slot. If data is not real, they will drop the incoming messages and generate new fake messages. This new fake message is transmitted in their time slot. Hence, real data will be delivered to origin ICH.
- After completion of data aggregation, circular routing is launched by origin ICH. In this, real data is distributed to other ICHs. One of the ICH will become 'sender' and this sender will deliver real data to sink. For this greedy routing algorithm is used.
- All interference clusters will be destroyed after data transmission. Again real source will determine new origin ICH and rebuild new ICHs and other routes.

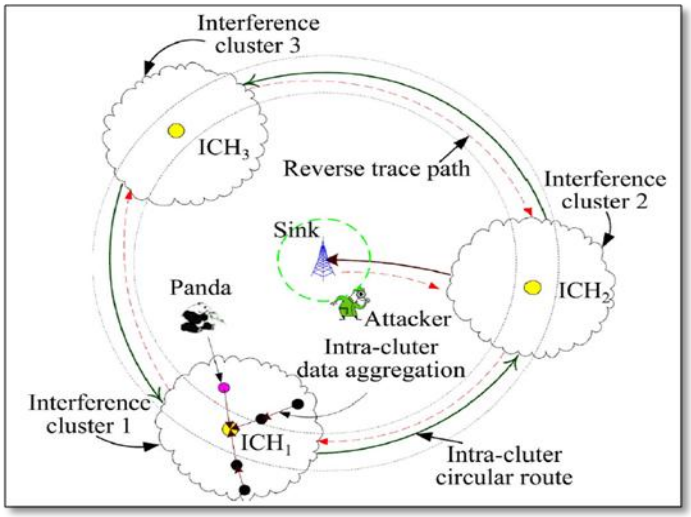

Fig 1- Multiple k-hop clusters based routing scheme

3.2 Multiple k-hop clusters based routing technique phases

The Multiple k-hop clusters based routing technique is classified into four phases. They are-

i. Interference cluster heads determination and clustering
ii. Intra cluster data aggregation

iii. Cyclic routing and delivering data to sink
iv. De-clustering and restarting

1. Interference cluster heads determination and clustering

In this first phase, the entire network is divided into several rings, interference cluster head is selected and then clustering is done. The division of network is done as per hop count from sensors to sink. The interference cluster head is selected by randomly picking a sensor which is located at 'p' hops i.e (0<p<k). The selected ICH is the origin ICH which is chosen by source node. The purpose of Interference cluster head (ICH) is to gather real data from sensors and launch circular routing to distribute real data to other ICHs till it reaches sink.

After selection of this origin ICH, there is need to launch circular routing to locate other remaining ∂-1 ICHs in the ring. The origin ICH launches circular routing. The interference clusters should be uniformly distributed. For this uniform distribution, firstly perimeter of IR is calculated i.e $l_i r$ and perimeter is divided into ∂ parts. Then, ICH is launched after every $l_i r/\partial$ hops in circular route. After determining ICHs, each ICH will form cluster with k hops.

2. Intra cluster data aggregation

The main idea of data aggregation is to combine data from different sources to eliminate redundant data transmissions and provide a rich and multi-dimensional view of the targets being monitored. In Intra cluster data aggregation, all cluster members only send data to their own ICH and data aggregation is performed at the every ICH, which helps to dramatically reduce transmission data and save energy.

TDMA hop by hop method is used to filter real data which is collected by ICH. If sensor receives real data, it stores real data and forward it to next hop in its time slot. If fake data packet is received, then it is dropped and new fake packet is generated in order to forward it to next hop. The following figure shows Intra cluster data aggregation in k hop cluster:

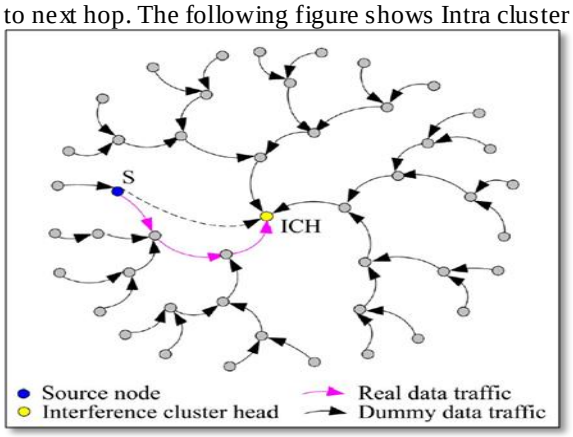

Fig-2 Intra cluster data aggregation in k hop cluster

3. Cyclic routing and delivering data to sink

After phase I and II, multiple interference clusters are established to confuse adversaries. To transmit the real data to sink, these clusters must be connected with each other. Hence circular routing is launched by origin ICH. The real data will be forwarded to all remaining ∂-1 ICHs till it reaches the target (sink).

After circular routing, randomly one of the ICH is picked. This ICH will become sender to deliver real data to sink. If adversary traces the path to IR, he will get confused because all the sensors in the cluster will be seen as fake sources. As ICH is randomly picked, constant single route will be changed every time. Hence it preserves the privacy from various attacks.

4. De-clustering and restarting

When the data reaches to sink, then source node will send notification of target to the origin ICH. After receiving notification, origin ICH will notify to other remaining ∂-1 ICHs to de-cluster. When all the ICHs get notification then de-clustering starts. Again the source node will determine new origin ICH and rebuild new ICHs and other routes by following MHCR scheme phases I, II and III. This is done to preserve privacy of location of source node.

3.3 Discussion

For preserving source location privacy, multiple k-hop clusters based routing technique is the best option. In this technique, the sensor network is divided into different rings and then the one node is selected as the Interference cluster head. This ICH launches circular routing to find out remaining ICHs. The clusters are formed and data aggregation is

done. All the data aggregation activity has been done within the cluster members and then Interference cluster head sends the real data packet to other remaining ICHs with the help of circular routing, till real data reaches the sink. Clustering method provides a reduction of redundancy and improvement over the lifetime of the wireless sensor network.
The overall flow of this method is as shown below:

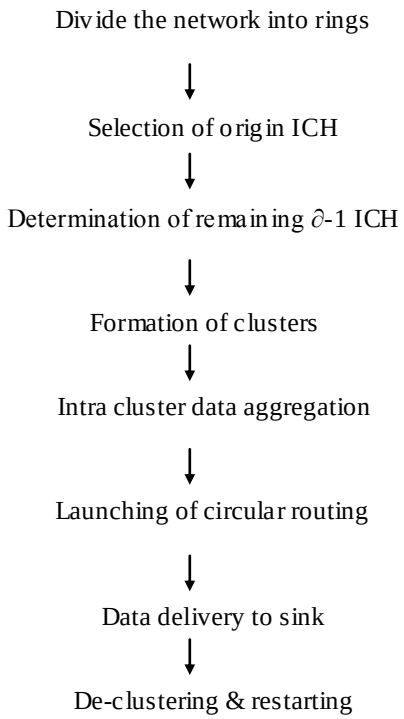

Fig 3- Flow of Multiple k-hop Clusters based routing technique

To prevent source location, multiple interference clusters are established which are used to conduct intra-cluster data aggregation before delivering data to sink. Each sensor in the cluster confuses adversaries. At the same time, these clusters are used to filter dummy traffic so that energy consumption is reduced. Moreover, circular route is established to connect interference clusters and hence real data is forwarded to sink.

The most important concept of intra-cluster data aggregation is used here. Intra-cluster data aggregation is the process of aggregating the data from multiple nodes present in particular cluster to eliminate redundant transmission and provide fused data to the sink. In this process, with the initial information the cluster heads in interference rings will start gathering data among their cluster members. The real source will send the real data to its cluster head and other cluster members turn into fake sources and then send dummy messages to their cluster heads.

Involvement of more number of nodes in intra-cluster communication leads to more confusion to the eavesdroppers, hence resulting into more privacy. But from the energy point of view, more fake source leads to more energy consumption in the network. In order to provide trade-offs between energy consumption and network security, randomly parts of the sensors are selected to generate dummy messages and these messages are send to their cluster heads, while cluster heads will then dump all the dummy messages they received and only keep the real message that was sent by a real source node. In this case, real event will be safely covered and real data will be successfully stored in the cluster heads of the interference ring.

After the data aggregation process, circular routing is launched. During this process, a cluster head receives the data will check if it holds the real data or not. If it holds real data then it will drop the fake data and send the real data to the next ICH, otherwise it will just relay the receiving data. Figures-4 shows the circular routing in a ring without or with a real event, respectively.

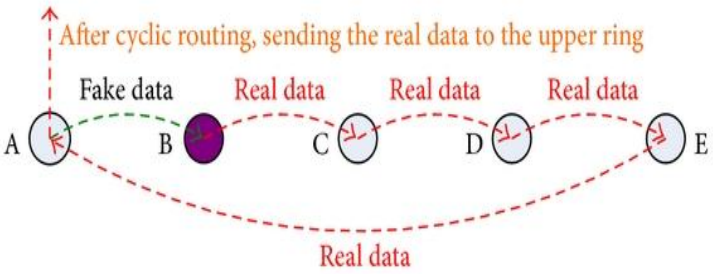

Fig 4- Circular route in the ring with real even.

The main aim of network is to monitor the target while the aim of the routing technique is to deliver the messages to sink, to enhance the location privacy of the source node and to provide efficient energy consumption. In multiple k-hop clusters based routing technique, multiple interference clusters are created with the help of residual energy to provide the security. If the δ interference clusters are generated then network security becomes ∂ times that of cloud based scheme. As every node in the cluster acts as a fake node, number of fake sources is same as number of sensor nodes present in the interference cluster.

CONCLUSION

The source location privacy is a significant issue in Wireless Sensor networks. Although there are various techniques that preserves the privacy of source location, but still there exits some problem in achieving privacy of source location. One solution to this problem is to use multiple k-hop clusters based routing technique. In this, network is divided into several rings and multiple clusters with size k-hop are formed. Each cluster has interference cluster head ICH which is selected by source node. The purpose of ICH is to form data aggregation among the cluster members and to send actual data to other ICHs through circular routing till it reaches the sink. As multiple interference clusters are formed, high privacy is achieved. Because each sensor node in the cluster acts as fake node so that adversaries get confused and cannot differentiate between actual source node and fake node. The energy consumption is also efficient as data filtering is done by ICH. ICH drops all fake packets and stores only real data with it. Network lifetime of MHCR technique is high than other techniques. Hence, MHCR technique surpasses the phantom routing technique and other routing technique in two aspects: privacy and network lifetime

REFERENCES

[1] Ren ju, Zhang yao-xue, Liu Kang ,"Multiple k-hop clusters based routing scheme to preserve source-location privacy in WSNs " Springer, 2014.
[2] Kamat P, Zhang Y,Trappe W, Ozturk c., et al., "Enhancing source-location privacy in sensor network routing" Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on. IEEE, 2005.
[3] Mehta K, Liu D, Wright M." Location privacy in sensor networks against a global eavesdropper" [C]// IEEE International Conference on Network Protocols, Beijing: IEEE, 2007: 314−323.
[4] Ozturk C, Zhang Y, Trappe W. "Source location privacy in energy-constrained sensor network routing" [C]// ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington: ACM, 2004, 25: 88−93.
[5] Li Y, Ren J. "Source-location privacy through dynamic routing in wireless sensor networks " [C]// IEEE International Conference on Communications, Cape Town: IEEE, 2010: 1−9.
[6] Li, Na, et al., "Privacy preservation in wireless sensor networks: A state-of-the-art survey" Ad Hoc Networks 7.8 (2009): 1501-1514.
[6] Long, J., et al. ,"Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks" Access, IEEE 2 (2014): 633-651.
[7]Mahmoud, Mohamed MEA, and Xuemin Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks" Parallel and Distributed Systems, IEEE Transactions on 23.10 (2012): 1805-1818.
[8] Li, Yun, and Jian Ren, "Preserving source-location privacy in wireless sensor networks" Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on. IEEE, 2009.

.