International Journal of Advance Research and Innovation
Vol. 3(1), Jan-Mar 2015, pp. 48-51
Doi: 10.51976/ijari.311508
www.gla.ac.in/journals/ijari
© 2015 IJARI, GLA University

Article Info
Received: 21 Jan 2015 | Revised Submission: 15 Feb 2015 | Accepted: 28 Feb 2015 | Available Online: 15 Mar 2015

Location Privacy and Lifetime Maximization using Low Energy Adaptive Technique in WSN

K. Jaisakthi and S. Nithyadhevi***

ABSTRACT

In a sensor network, an important problem is to provide privacy to the event detecting sensor node and integrity to the data gathered by the node. In the privacy preserving location monitoring system for wireless sensor networks can be design to enable the system to provide high quality location monitoring services for system users, while preserving personal location privacy. Hybrid Cluster Structure (CS) used for sensor networks to improve the lifetime by using Low Energy Adaptive (LEA) protocol. The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using Cluster Structure. All CHs are interconnected in CS mode to transmit data to sink. Hybrid Cluster Structure (CS) used for sensor networks. The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using Cluster Structure.CH can be select by using stochastic algorithm. All CHs are interconnected in CS mode to transmit data to sink.

Keywords: *Wireless Sensor Networks; Source Location Privacy; Network Lifetime; Cluster Structure; Hierarchical Routing.*

1.0 Introduction

Source location privacy is to hide the physical location of the message source and makes it more difficult for an adversary to trace messages back to the source location. Considering a mission critical military application, any leakage of information such as event location or time can prove beneficial to the adversary and costly to the network goal. Location privacy can be achieving by using multiple diversionary routing scheme. Energy consumption of the sensing device should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime. Lifetime of networks depends upon the energy consumption of the hotspot or known as energy hole. If the increased energy consumption is not in the hotspot, the network lifetime will not be affected. The main contribution of this work is to better preserve source location privacy while at the same time keeping network lifetime unaffected by minimizing the energy consumption in hotspots and fully using residual energy of light load regions to establish many routes as possible. The numbers of clustering algorithms have been proposed to improve the lifetime of the sensor network. In clustering, the sensor network is divided into clusters and then the one node from each cluster is selected as the cluster head. All the data aggregation activity has been done within the cluster and then cluster head use to send the information of a particular cluster to the BS which is also known as sink node. Clustering method provides a reduction of redundancy and improvement over the lifetime of the wireless sensor network.

LEA is known as a distributed hierarchical protocol. It provides the aggregation for data in wireless sensor networks by selection of Cluster heads in random manner. This protocol first judges the strength of the received message or signal and then formation of cluster takes place. In this Cluster Head nodes are taken as routers to reach the sink node. Every non- Cluster Head node sends its data to their CHs. Before sensing received information to sink, CHs aggregate the information. The operation of LEA is conducted in numerous rounds, and each round is separated into two phases known as the setup phase and the steady state phase. In the setup phase the various clusters of sensor network are organized, while in the steady state phase information is delivered to the sink node.

**Corresponding Author: Department of Computer Science Engineering, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Anna University, Chennai, India (E-mail: jaisakthi.26@gmail.com)*
***Department of Computer Science Engineering, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Anna University, Chennai, India*

During the setup phase, each sensor node decides whether or not to act as a cluster head for that particular round. This decision is made by the sensor node by randomly selecting a number between 0 and 1.

2.0 Related Work

Bicakci, et al. [1] introduced a filtering scheme called OFS (Optimal Filtering Scheme) to maximize the network lifetime and preserve event Unobservability against global eavesdroppers. However, for the global eavesdroppers, the existing works have certain limitations. Since all nodes are sending a large number of fake packets, which will not only greatly increase the energy consumption f nodes and reduce the network lifetime, but also increase the probability of packet collisions and reduce the efficiency of packet transmission. It still remains as an open problem.

Chen. H, et al [2] proposed four location privacy protection schemes are called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively. Kamat. P, et al. [3] developed a phantom routing technique for flooding as well as single path routing. It involves taking a random walk before forwarding the packet towards the base station in an attempt to increase the complexity of the adversary to backtrack to the source. Although the schemes are robust, they have a large overhead involved and may not with stand attacks under a collaborative adversary model. Leeke. M, et al. [4] presents a fake source technique. It works as follows: Whenever a real source node sends a message to the sink, another node, known as the fake source, will similarly send a message the sink so as to confuse an attacker as to the location of the asset. But it has a drawback that is an adversary may perform hop by hop trace back to the source location. Li. X, et al. [5] presents a scheme to hide source information using cryptographic techniques incurring lower overhead. The packet is modified by dynamically selected nodes to make it difficult for a malicious entity to trace back the packet to a source node and also prevent packet spoofing. But it does not support against context based privacy threats. Mehta. K, et al. [6] presents two techniques: namely periodic collection and source simulation to wade off global eavesdropping attack. The source simulation technique is similar to fake source technique. The weakness in case of periodic collection type technique is the latency incurred as well as overhead, while in source simulation.

Y. Yang, et al. [7] presents event source Unobservability, which promises that a global adversary cannot know whether a real event has ever occurred even he is capable of collecting and analyzing all the messages in the network at all the time, it uses chosen dummy traffic to hide the real event sources in combination with mechanisms to drop dummy messages to prevent explosion of network traffic. But it has the drawback of having overhead due to dummy packet generation.

2.1 Power efficient gathering in sensor information systems (PEGASIS)

In this protocol [9], some chains consisting of different sensor nodes have been formed. Every node sends its data to the neighbor sensor node and most appropriate node is selected to transmit the data to the sink node. PEGASIS does not follow the concept of cluster formation and it prefers to decide or choose only one node from the chain to transmit to the sink node instead of using multiple sensor nodes present in the network. When a sensor node fails due to low battery backup, again the chain is made using the same previous greedy approach.

2.2 Hybrid, energy-efficient, distributed clustering approach (HEED)

HEED [10] is also a distributed clustering algorithm used for Wireless Sensor Networks. Every sensor node has some amount of energy associated with it. This energy of nodes reduces during reception and transmission of data. It also access query requests coming from the Base Station. HEED protocol follows to circulate the role of server among all nodes of the cluster so that a balance will be maintained between residual energy of all nodes of the cluster. Hence, remaining energy of cluster head would not drop to minimum leading to less node failures due to energy depletion in the network.

3.0 System Model

3.1 Network lifetime maximization

Data Gathering in wireless sensor network is challenging process, since the more data transmission will reduce network efficiency and not able to get long time energy level for network life. To resolve this, lot of approach handled like dynamic hotspot, hierarchical structure, tree based routing techniques etc. Clustering method uses hybrid CS for sensor networks.

The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using CS. CHs use CS to transmit data to sink. Proposed systems analytical model studies the relationship between the size of clusters and number of transmissions in the hybrid CS method to find optimal size of clusters that can lead to minimum number of transmissions. Hybrid Cluster Structure (CS) used for sensor networks.

Fig 1: Overview of CH Determination

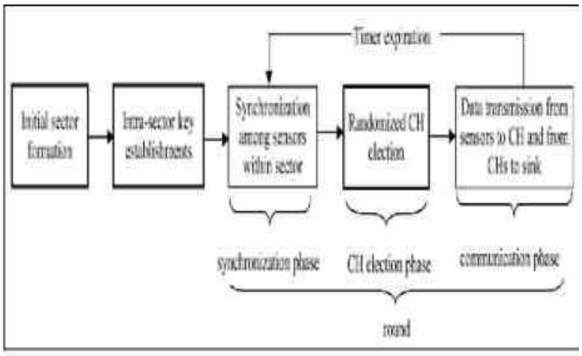

Timer expiration
Initial sector formation
Intra-sector key establishments
Synchronization among sensors within sector
Randomized CH election
Data transmission from sensors to CH and from CHs to sink
synchronization phase
CH election phase
communication phase
round

Fig 2: LEA Clustering

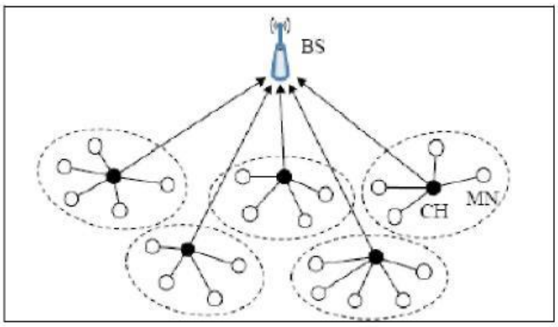
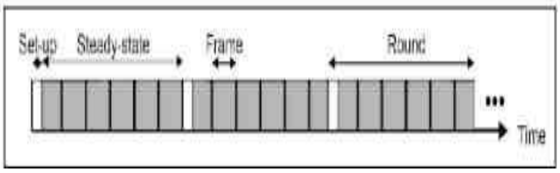


Fig 3: Operation of LEA Protocol



The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using Cluster Structure. All CHs are interconnected in CS mode to transmit data to sink. This scheme has an issue that is CH will fail in data accusation when it does data gathering in long time. If CH failed or lose its energy, then a particular cluster only will be partitioned from entire network. The solution to this issue is to propose Low-Energy Adaptive (LEA) protocol.

The operation of this protocol consists of two phases:

- Setup Phase
- Steady state Phase

3.1.1 Setup phase

The clusters are organized and the cluster heads are selected. The cluster heads aggregate, compress and forward the data to the base station. Each node determines whether it will become a cluster head, in this round, by using a stochastic algorithm at each round. If a node becomes a cluster head for one time, it cannot become cluster head again for P rounds.

Here P is the desired percentage of cluster heads. Thereafter, the probability of a node to become a cluster head in each round is 1/P. This rotation of cluster heads leads to a balanced energy consumption to all the nodes and hence to a longer lifetime of the network. Figure-3 shows the operation of LEA protocol.

3.1.2 The steady state phase

The data is sent to the base station. The duration of the steady state phase is longer than the duration of the setup phase in order to minimize overhead. Moreover, each node that is not a cluster head selects the closest cluster head and joins that cluster. After that the cluster head creates a schedule for each node in its cluster to transmit its data.

3.1.3 Stochastic algorithm

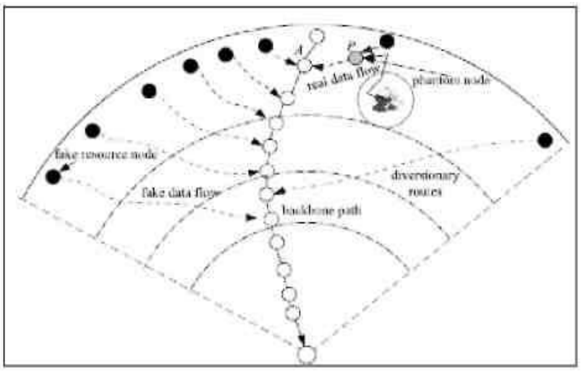
A stochastic algorithm is referred in each round by every single sensor node to determine whether it can be a cluster head for that particular round or may not act as a cluster head for that round. All normal nodes of the cluster communicate with CH in TDMA fashion which is scheduled by CH.

3.2 Source location privacy

In existing scheme, data of phantom node is sent to the sink according to the shortest routing protocol, therefore the adversaries can trace back to the phantom node.

They cause extra energy consumption to sensor nodes, which could shorten the network lifetime. A tree based diversionary routing scheme creates more diversionary routes which greatly improves source location privacy.

Fig 4: Overview of Source Location Privacy



At the same time, the network lifetime does not deteriorate with the increase number of diversionary routes compared with the traditional routing protocol. A fake source node can be created near the real source node. Packets are sending via this fake node. Dummy packets also sent to sink. By this dummy transmission make confusion to adversary. Server can monitor all the nodes activities. Sensor nodes present in the real routing path can send alerts to the server. Server can act as a backbone. It can be monitoring all of the node's activities. Establish all possible routing paths from the source to destination with the same length. Adversary cannot find the real source node via the shortest path reverse tracing method. Create fake source node near the real source node. Transmit packets via this fake node. Data packets can be encrypted before transmitting. So intruder may not easily extract the information.

4.0 Conclusion

This scheme has a strong resistance to reverse trace of the adversary. The route structure is homogeneous, so the adversary cannot speculate the phantom node and source of data. The system can provide reliable responses to queries while minimizing the use of limited energy and computational resources. This data storage scheme ensures scalability and load balancing of communication as well as adaptively in presence of dynamic changes of CH. To minimize the load of the network, minimum number of cluster heads has been elected in each transmission round. The simulation results will show that our proposed LEA protocol increases network lifetime.

References

[1] K. Bicakci et al., Maximizing lifetime of event unobservable wireless sensor networks, IEEE Commun. Lett, 15(2), 2011, 205_207

[2] H. Chen, W. Lou, Protecting end to end against local eavesdropper in wireless sensor networks, Pervas. Mobile Comput, 2014

[3] P. Kamat. et al., Enhancing source-location privacy in sensor network routing in Proc. 25th IEEE. Int. Conf. Distrib Compute. Syst, Columbus, OH, USA, 2005, 599-608

[4] M. Leeke, S. Shrestha, On the use of fake sources for source location privacy: Trade-offs between energy and privacy, 2011

[5] X. Li et al., Maintaining source privacy under eavesdropping and node compromise attacks, in Proc. IEEE INFOCOM, Shanghai, China, 2011, 1656-1664

[6] K. Mehta et al., Location privacy in sensor networks against a global eavesdropper, in Proc. IEEE Int. Conf. Netw. Protocols (ICNP), 2007

[7] Y. Yang .et al., A cloud-based scheme for protecting Source location privacy against hotspot-locating attack in wireless sensor network. IEEE Trans. Parallel Distrib. Syst, 23(10), 2012, 1805-1818

[8] J. Wu, S. Yang, Coverage and Connectivity in Sensor Networks with Adjustable Ranges, International Workshop on Mobile and Wireless Networking (MWN), 2004

[9] S. Lindsey, C. S. Raghavendra, PEGASIS: Power efficient Gathering in Sensor Information System Proceedings, IEEE Aerospace, Conference, 3, Big Sky, MT, 2002, 1125-1130

[10] P. Neamatollahi, H. Taheri, M. Naghibzadeh, Mohammad-Hossein Yaghmaee, A Hybrid Clustering Approach for Prolonging Lifetime in Wireless Sensor Networks, International symposium on computer networks and distributed systems, 2011, 170-174