International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

# IMPROVED DEVELOPMENT OF ENERGY EFFICIENT ROUTING ALGORITHM FOR PRIVACY PRESERVATION OF SINK IN WSN

**Pallavi Saxena[1], Dr. Kanika Sharma[2]**

[1] *ME Scholar, E&C Department, NITTTR, Chandigarh, India*
[2] *Associate Professor, E&C Department, NITTTR, Chandigarh, India*

---

**Abstract** - ***A wireless sensor network (WSN) is a distributed network that facilitates wireless information gathering within a region of interest. For this reason, WSNs are relied upon by the Department of Defense for deployment in remote and hostile areas. The information collected by sensors is aggregated at a central point known as a sink node. Two challenges in the deployment of WSNs are limited battery power of each sensor node and sink node privacy/anonymity. The role played by the sink node raises its profile as a high value target for attack, thus its anonymity is crucial to the security of a WSN. In order to improve network security, a protocol is implemented that conceals the sink node's location while being cognizant of energy resource constraints. In this thesis, a routing algorithm based on node clustering is developed to improve sink node anonymity while simultaneously limiting node energy depletion. Via MATLAB simulations, the effectiveness of this algorithm in obfuscating the sink node's location in the WSN while preserving node energy is analyzed. It is shown that the anonymity of the sink node is independent of traffic volume and that the average energy consumed by a node remains consistent across topological variations.***

***Key Words:*** *RRHA, SPIN, CH, LPR, AVGEC, MAXEC, MINEC.*

## 1. INTRODUCTION

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the first wireless local area network standard, named IEEE 802.11 [1]. The practical advantages of being able to move away from a wired architecture have driven staggering growth in the development of consumer and commercial devices that are able to connect wirelessly. Substantial improvements in integrated chips have also contributed to the miniaturization of devices, an increase in processing power resident in a device, and a rather dramatic reduction in cost per device.

Due to these technological advances, the manufacturing of small and low cost sensors has become technically and economically feasible [2]. A sensor observes an event or gathers some physical data from its area of interest. It then processes the observed or gathered data using a tiny embedded processor. The sensor sends the processed data to a central data collector either through direct wireless transmission or through intermediate nodes [3]. A basic sensor is composed of four subsystems: power, sensing, processing, and communications. The interaction of these four subsystems is illustrated in Figure 1.1. The power subsystem is a small battery with finite power capacity that is responsible for supporting the functions of all of the other subsystems. The capabilities of the sensing subsystem are very broad and can be tailored for desired applications. The sensing subsystem can be employed to gather meteorological variables such as temperature or pressure or for military use in surveillance missions to detect moving targets [3]. A small processor in the sensor comprises the processing subsystem. The processor is responsible for preparing sensed data for transmission. The communication subsystem is a Radio Frequency (RF) transceiver which is responsible for transmitting data from the sensor and receiving information from other sensors in the WSN. The Sensors may have additional optional subsystems, such as Global Positioning Systems (GPS) or mobilizers [2].

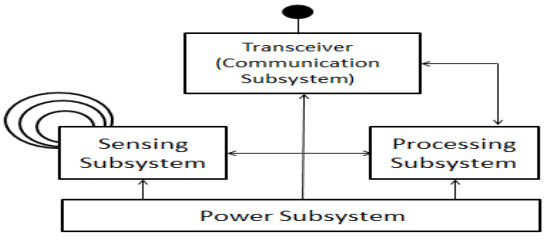


**Figure 1:** The basic architecture of a sensor.

## 2. WIRELESS SENSOR NETWORKS

A wireless sensor network (WSN) is typically composed of a set of sensors that probe their physical environment for information and report their measurements to a nearby central controller. The controller aggregates all of the sensor node's information and interfaces the WSN to remote users who use the information to plan specific actions [5]. WSNs are ad-hoc networks in which sensor nodes are widely distributed in a region of interest for data extraction in real time. The sensor nodes act as both sensing and routing devices. Multiple sensor nodes may be used to transmit data from the initial source node to the destination (i.e., multi-hop communication). The destination node in a WSN is characterized as a sink node. A representative WSN topology for military applications is illustrated in Figure 1.2.

When a WSN is deployed, each sensor has a finite amount of energy. Sensors are powered by the power subsystem, and every action that is taken by a sensor has an energy cost that slowly depletes the sensor's power. Some actions like communication require a large amount of power, while other actions like processing and sensing data require a very small amount of power. When a sensor loses power, it is no longer able to sense information, communicate with other nodes or route information. The death of a single node does not have a major impact on the WSN, but as additional nodes die out, the performance of the WSN is degraded as the network may become partitioned and is no longer reliable. The tradeoff associated with small and inexpensive devices is that the network itself is resource constrained and has a limited lifetime.

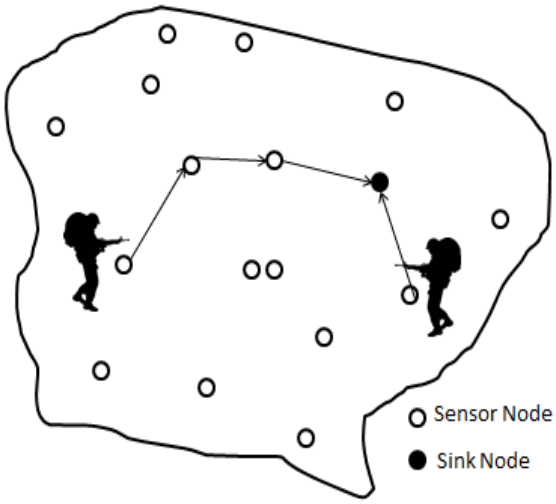


Figure 2: The basic topology of a WSN

## 3. PRIVACY IN WIRELESS SENSOR NETWORKS

To defend and protect a WSN, it is necessary to understand the layering architecture of a network. A high degree of cooperation and coordination is needed for successful interactions between sensors. These interactions are complex and must be broken down into subtasks which are implemented separately [11]. The layering architecture of a network facilitates the implementation of these subtasks. The most common network layering model is based on the Open Systems Interconnection (OSI). The general network layering construct based off of the OSI model is shown in Figure 1.3. The architecture that defines the network functionality is split into layers that collectively form the protocol stack of the network [12]. Each layer in the stack performs a related subset of the functions required to communicate with another system. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts between sensor nodes [13].

### 3.1 Sink Node Approaches

The challenge of location privacy for the sink node is that the network traffic is asymmetric, with nodes further from the sink node seeing dramatically less traffic than nodes within immediate range of the sink node.

#### *3.1.1 Deceptive Packets*

Deceptive packets are generated from low traffic volume sensor nodes and take care to avoid routing through high traffic areas, ending their transmission at another low traffic volume node [5]. The deceptive packets protocol assumes that the adversary is conducting traffic analysis within the WSN and is able to correlate data transmissions to determine the end to end path. The Belief is a value which denotes the adversary's confidence that the destination node is the sink node [5]. The goal of using deceptive packets is to make the belief values of other nodes similar to or higher than the sink node. This approach is similar to the source simulation approach for source-location privacy. The two are differentiated by the method to generate these deceptive packets. Unlike source simulation where the nodes generating false traffic are seeded prior to deployment of the WSN, the deceptive packets protocol is adaptive. Sensor nodes use online data processing to evaluate the belief value for each node and determine where traffic should be generated from and where it is destined to go.

A disadvantage to the deceptive packet approach is that its performance is highly variable. In order to evaluate the belief values, the adversary must analyze the data it has collected. Deceptive packets utilize online processing to mimic the adversary's belief calculations and determine where additional traffic should be generated. If the adversary is calculating the belief values at a different rate than the additional deceptive packets are being generated, then it is possible that the adversary

may not be foiled by the deceptive packets. The largest limitation of this is that there is a significant amount of communication overhead associated with evaluating the belief and adjusting the volume and location of the deceptive packets. It is difficult to optimize minimizing communications overhead and normalizing the belief value of multiple nodes.

### *3.1.2 Location Privacy Routing*

In the Location Privacy Routing (LPR) protocol, each sensor divides its neighbors into two lists: a closer list consisting of neighbors who are closer to the sink node, and a further list consisting of neighbors that are further from the sink node. When a sensor forwards a packet, it randomly selects a neighbor from one of the two lists. The route for multiple messages originating from the same source node is not always the same because the next hop is randomly selected. The two lists make it more difficult to predict the next hop and direction of the sink node because traffic does not always travel in the cardinal direction of the sink node [16]. Ultimately, this means that an adversary who is conducting a packet tracing attack has to take many more hops before reaching the sink because it is frequently deviated in the wrong direction.

If LPR is applied alone, the protection for location privacy is not significantly strong. This is because the overall traffic trend in the network still points towards the sink node. Although this problem can be alleviated by increasing the probability that a sensor forwards to a neighbor on the further list, it leads to a longer delay and higher energy costs [16].

One way to overcome this is to combine LPR with fake packet injection similar to deceptive packets. The basic idea of fake packet injection is that when a sensor node forwards a real data packet, it may generate a fake packet and transmit it to a neighbor randomly chosen from the further list. This leads an adversary away from the sink node, distributes the direction of outgoing packets while reducing data latency for real data, and increases the location privacy of the sink node in the WSN. These methods complement one another but are ultimately challenged by a global adversary who can see that all real messages ultimately always arrive at the sink while fake messages do not.

### *3.1.3 k- anonymity*

The goal of the k-anonymity algorithm is that at least k entities exhibit the same characteristics as nodes located close to the sink. In order to achieve k-anonymity, a Euclidian minimum-spanning tree-based routing algorithm is proposed to route traffic so that traffic volumes are equally high at k sensor nodes in the WSN. Since at least k nodes exhibit similar traffic statistics, an adversary trying to locate the sink node has to locate and inspect all nodes within the communication range of each node [10].However, positioning k designated nodes within the WSN is complex as it affects two conflicting goals: the routing energy cost and the achievable privacy level [10]. This is ultimately an optimization problem which requires prioritizing one goal or the other.

### *3.1.4 Randomized Routing with Hidden Address*

The methods discussed thus far have assumed a passive adversary whose methods are limited to observing network traffic. An active attacker can compromise a node and read the header field of a packet to identify the receiver. The Randomized Routing with Hidden Address (RRHA) scheme keeps the identity of the location of the sink secret in the network. Sensors do not know who and where the sink is when routing packets and do not specify a destination when reporting their measurements. The packets are forwarded along different random paths for a specified path length and are then discarded when the length is reached [17].

The random path taken by RRHA introduces some packet delay. The longer a packet lingers in the WSN, the more energy it consumes. When there is high traffic volume, the delay caused by the random paths can accumulate to cause significant network congestion, exaggerating the delay further and degrading the performance. The major limitation of RRHA is that it cannot guarantee that the sink will receive the data. Simulations showed that the longer the path length, the higher the success rate of information reaching the sink [17]; however, in many time sensitive applications this is clearly an unsatisfactory outcome.

## 4. ENERGY CONSERVATION IN WIRELESS SENSOR NETWORK

Energy conservation in a WSN is a crucial issue as sensor nodes are all powered by limited battery sources. Sensors utilize their energy for sensing and processing data as well as transmitting and receiving data. The communication subsystem of a sensor node consumes more energy than the processing subsystem. It has been shown that transmitting one bit of data may consume as much energy as executing a few thousand computational instructions [19]; thus, it is important that energy efficiency be targeted towards the communications subsystem as only minimal gains are attained by optimizing the energy of the sensing and processing subsystems. In order to develop energy efficient communication mechanisms in a WSN, focus is made on the network layer of the protocol stack. Efficient algorithms can be developed at the network layer such that reliable route setup and relaying of data

from the sensor nodes to the sink is achieved and the lifetime of the network is maximized [7].

## 5. CLUSTER BASED ROUTING TO ACHIEVE ANONYMITY

There is a substantial amount of ongoing research in the fields of both privacy and energy conservation in WSNs. In order to achieve energy constrained anonymity, a routing algorithm based on node clustering which results in at least n other nodes having similar observable traffic statistics, thus obfuscating the sink node's location is proposed.

The steps that the WSN takes upon deployment to route traffic are as follows:

- CH election and cluster formation.
- Choose a subset of the CHs to serve as broadcast CHs.
- CHs use Dijkstra's algorithm to determine their route to the sink node's CH.

### *5.1 CLUSTERING*

Clustering is a standard approach for achieving efficient and scalable performance in sensor networks. Clustering nodes into groups saves energy and facilitates distribution of control over the network [20]. To form clusters, sensor nodes must first elect a CH for each cluster. Nodes in the WSN which are not CHs find the closest CH within range and become cluster members. The nodes in a cluster only communicate with one another and the CH. Data sensed by a node is transmitted to its CH. The CH is responsible for all routing and communication external to the cluster. This yields energy savings over a "flat" topology, where each node must determine the route from source to sink node. For these reasons, the first step in our proposed algorithm is the initialization and formation of clusters. All of the nodes in the WSN either elect to become a CH or join a cluster as a cluster member, with the exception of the sink node. The sink node is always a cluster member in the WSN; it is never elected to be a CH. The constraint on the sink node is forced because, if the sink node is always a CH, then it becomes clear to an adversary conducting traffic analysis that after a few CH rotations the sink node is the only node constantly re-elected to the role of CH. This leads the adversary to conclude the sink node (one of several CHs) has a more significant role in the WSN.

## 6 PROPOSED ALGORITHM

Based on the proposed Methodology , the routing algorithm consists in the following steps.

1) The nodes are randomly distributed throughout the entire area of interest. The sink node is placed at the location (x,y) =(25m ,75m).

2) Initialization and formation of clusters. All of the nodes either elect to become cluster head or join as a cluster member .

3) Cluster heads are rotated to distribute the burden of being cluster head across the WSN.CHs are rotated when either one of the CHs have expanded a certain amount of energy or a specific number of messages have been transmitted through the WSN.

4) CHs are chosen to broadcast. The sink node's CH always broadcasts the message it receives so that the sink node can receive the information.

5) To choose the broadcast CH, the CHs are ordered by their residual energy levels.

6) To establish routing paths, each CH uses Dijkstra's routing algorithm to determine the path to the sink node's CH.

7) Euclidian distance is used as the cost between the two CHs in Dijkstra's routing algorithm.

8) Sink node anonymity is calculated for the broadcast nodes.

## 7. RESULTS AND DISCUSSIONS

### 7.1ANALYSIS OF TOPOLOGY 1

The physical location of the nodes remains the same throughout Topology 1. Across the five trials at each simulated traffic volume, the only thing that changes is the role each nodes plays in the WSN.

**Figure 6.1 The average energy consumed increases as traffic volume increases in all five trials in Topology1.**

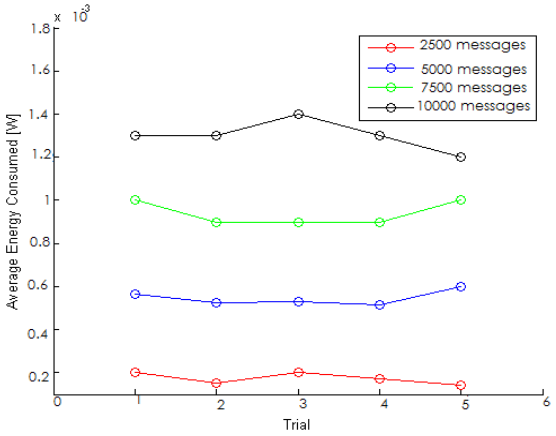


Fig7.1**The average energy consumed increases as traffic volume increases in all five trials in Topology1**.

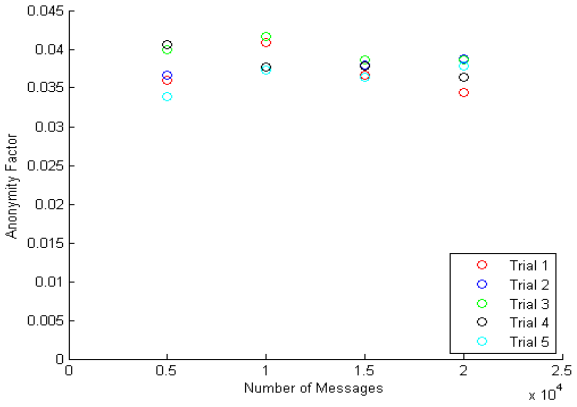


Fig-7.2: **The anonymity factor of each trial at each traffic volume for Topology 1.**

## 7.2 ANALYSIS OF TOPOLOGY 2

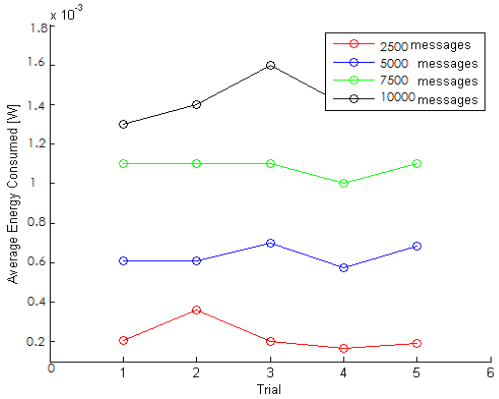


Fig-7.3: **The average energy consumed increases in all five trials for topology 2.**

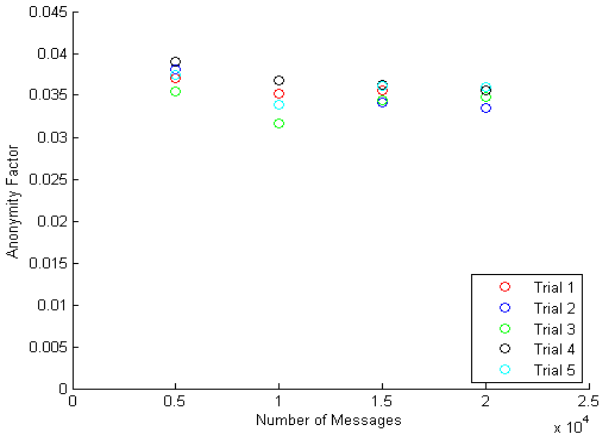


**Fig7.4** The anonymity factor of each trial at each traffic volume for topology 2.

## 7.3 ANALYSIS OF TOPOLOGY 3

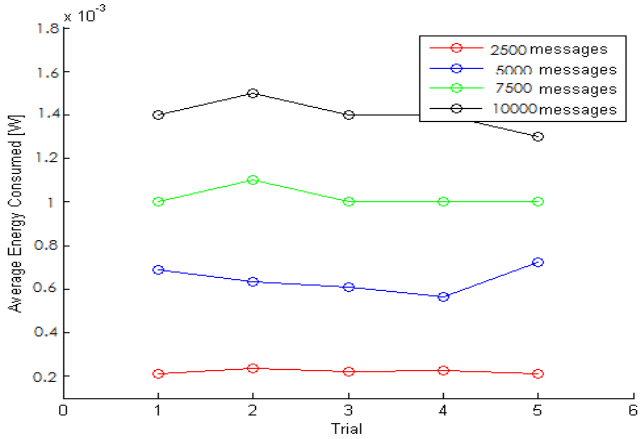


Fig-7.5: **The average energy consumed increases as traffic volume increases in all five trials in Topology 3.**

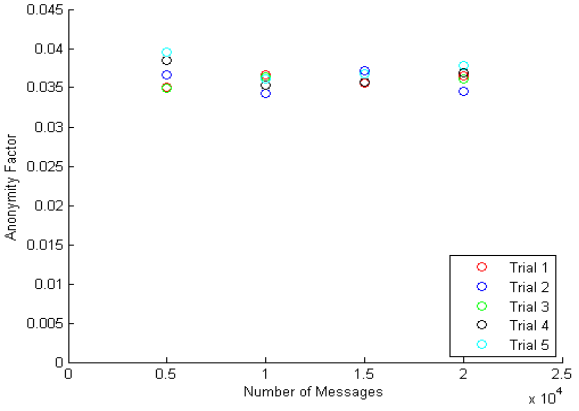


Fig-7.6: **The anonymity factor of each traffic volume for topology 3.**

**The value of anonymity factor for each topology is under 0.04.The value of average energy for all topologies is given in table below.**

| Average energy | |
|---|---|
| 2500 messages | $2.20x10^{-4}$ |
| 5000 messages | $6.08x10^{-4}$ |
| 7500 messages | $1.02x10^{-4}$ |
| 10000 messages | $1.37x10^{-4}$ |

**Table- 7.1 :** Average energy consumed

## 8 CONCLUSIONS

WSNs can be used for a variety of military, civilian and commercial applications. This thesis was motived by the proliferation of WSNs for military applications. The existing research focused on energy conservation without concern for WSN privacy or WSN privacy without concern for the limited resources of a WSN.

The existing research in both the privacy and energy conservation fields look for contributions from both fields which could be brought together to develop a routing algorithm that holistically addresses the especially vital issue of sink node privacy/anonymity in a resource efficient manner.

## REFEERENCES

[1] M. Conti, "Body, personal and local ad hoc wireless networks," in The Handbook of Ad Hoc Wireless Networks, M. Ilyas , Ed. Boca Raton, FL: CRC Press, 2003

[2]J.N Al-Karaki and A. E. Kamal, "Routing techniques in Wireless Sensor Networks: A survey," IEEE Wireless Communications, Vol. 11, No. 6, Page(s):6–28, 2004.

[3]A. Rahman et al., "A survey on energy efficient routing techniques in Wireless Sensor Network," in 15th International Conference on Advanced Communications Technology, Page(s):200–205, 2013.

[4]K. A. White, "Tactical Network load balancing in multi-gateway Wireless Sensor Networks," M.S. thesis, Department of Electrical and Computer Engineering, Naval Post Graduate School, Monterey, CA, 2013.

[5]Y. Ebrahimi and M. Younis, "Using deceptive packets to increase base station anonymity in Wireless Sensor Network," in Proc. Wireless Communications and Mobile Computing Conference, Page(s):842–847, 2011.

[6]M. Shao et al., "Towards statistically strong source anonymity for sensor networks," in Proc. IEEE Conference on Computer Communications, Page(s):466–474, 2008.

[7]N. P. Karthickraja and V. Sumathy, "A study of routing protocols and a hybrid routing protocol based on rapid spanning tree and cluster head routing in wireless sensor network," in Proc. IEEE International Conference on Wireless Communications and Sensor Computing, Page(s):1–6, 2010.

[8] J. Kulik et al., "Negotiation-based protocols for disseminating information in Wireless Sensor Networks," *Wireless Networks*, Vol. 8, No. 2, Page(s):169–185, 2002.

[9]K. Mehta, D. Liu and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, Vol. 11, No. 2, Page(s):320–336, 2012.

[10]G. Chai et al., "Enhancing sink-location privacy in wireless sensor networks through k-anonymity," International Journal of Distributed Sensor Networks, Page(s):1-16, 2012.

[11]W. Stallings, "Data communications, data networks, and the Internet," in Data and Computer Communications, 9th ed., Upper Saddle River, NJ: Prentice Hall, Page(s):170–185, 2011.

[12]C.-H. Wu and J. D. Irwin, "An introduction to information networks," in Introduction to Computer Networks and Cyber Security. Boca Raton, FL: CRC Press, Page(s):99-105, 2013.

[13]I. F. Akyildiz et al., "A survey on sensor networks," IEEE Communications Magazine, Vol. 40, No. 8, Page(s):102–114, 2002.

[14]X. Chen et al., "Sensor Network Security: A Survey," IEEE Communications Surveys and Tutorials, Vol. 11, No. 2, Page(s):52-73, 2009.

[15]K. Mehta, D. Liu and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," in IEEE

International Conference on Network Protocols, Page(s): 313-323,2007.

[16]Y. Jian et al., "A novel scheme for protecting receiver's location privacy in wireless sensor networks," IEEE Transactions on Wireless Communications, Vol. 7, No. 10, Page(s): 3769-3779, 2008.

[17]Audrey F. Callanan and Preetha Thulasiraman," Achieving Sink Node Anonymity Under Energy Constraints in Tactical Wireless Sensor Networks ",IEEE International Multidisciplinary conference Cognitive methods In situation awareness and decision support, Page(s):186-192, 2015.