



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

NPS Scholarship

Publications

---

2015

## Achieving Sink Node Anonymity Under Energy Constraints in Tactical Wireless Sensor Networks

Callanan, Audrey F.; Thulasiraman, Preetha

IEEE

---

Callanan, Audrey F., and Preetha Thulasiraman. "Achieving sink node anonymity under energy constraints in tactical wireless sensor networks." Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2015 IEEE International Inter-Disciplinary Conference on. IEEE, 2015.

<https://hdl.handle.net/10945/59380>

---

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

*Downloaded from NPS Archive: Calhoun*



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

<http://www.nps.edu/library>

# Achieving Sink Node Anonymity Under Energy Constraints in Tactical Wireless Sensor Networks

Audrey F. Callanan\* and Preetha Thulasiraman†

\* United States Naval Academy, Annapolis, MD, USA  
callanan@usna.edu

† Naval Postgraduate School, Monterey, CA, USA  
pthulas1@nps.edu

**Abstract**—A wireless sensor network (WSN) is a distributed network that facilitates wireless information gathering within a region of interest. The information collected by sensors is aggregated at a central node known as the sink node. Two challenges in the deployment of WSNs are limited battery power of each sensor node and sink node 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, we must implement a protocol that conceals the sink node's location while being cognizant of energy resource constraints. In this paper we develop a routing algorithm based on node clustering to improve sink node anonymity while simultaneously limiting node energy depletion. Via MATLAB simulations, we analyze the effectiveness of this algorithm in obfuscating the sink node's location in the WSN while preserving node energy. We show 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.

## I. INTRODUCTION

A wireless sensor network is typically composed of a set of sensors that probe their physical environment for information and report their measurements to a nearby central controller, also known as the sink node. They 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 sink node aggregates all of the received data and transfers it to a command and control site.

WSNs greatly extend the Department of Defense's (DOD) ability to monitor and control the physical environment from remote locations and improve the accuracy of information obtained via collaboration among sensor nodes and online information processing at these nodes [1]. For this reason, WSNs are currently used for a broad range of military, civilian, and commercial applications. Remote sensors provide a means to economically conduct continuous surveillance of vast areas, contributing key information to the intelligence collection effort.

WSN security is especially important from the DOD perspective. An important aspect of WSN security is the ability to protect the sink node. The sink node in a WSN is crucial for

gathering, aggregating, and transferring sensor information. In terms of military applications, the sink node is relied upon to provide critical information to personnel on the ground about an area of interest. Since the sink node is a central point of failure, an adversary can destroy the sink and render ineffective the data gathering duties of the entire sensor network. Thus, failure to protect the network completely subverts the intended purpose of sensor network applications [2]; therefore it is important to implement specific protocols that conceal the sink node's location.

### A. Research Motivations and Contributions

Our study into WSNs is from a security perspective in that, because these networks are remotely deployed, they are vulnerable to malicious infiltration. The growing capabilities of WSNs and any potential adversary require some modification of the tactics, techniques and procedures used for the tactical employment of WSNs. It can no longer be assumed that an adversary has to be technologically advanced to observe or interfere with a deployed WSN. Due to the shared nature of wireless communication media, an attacker can easily eavesdrop on the radio communications either by purchasing their own sensor devices or by leveraging other radio devices capable of monitoring message transmission. Thus, no matter whether messages are encrypted or not, an adversary is able to identify contextual information [3]. While all traffic in a military wireless sensor network is encrypted, the contextual information that is revealed is meaningful—where the communication occurred and who participated in the communication. The role played by the sink node in the sensor network raises its profile as a high value target for attack; thus, sink node anonymity is crucial to the security of a wireless sensor network deployed for tactical use.

The anonymity of the sink's location is a unique problem in WSNs. Most security and privacy research related to WSNs focuses on secure routing, key management, source privacy and denial of service. Nevertheless, the protection of the sink's location cannot be achieved using existing security mechanisms such as packet encryption, key management, etc. At the same time, a scheme for sink protection should not affect normal sensing and communication tasks that require knowledge of the sink's location. In most cases, sensed data is transmitted along paths from source nodes to a sink node. This

produces pronounced traffic patterns that reveal the direction and, thus, the location of the sink node. An adversary can analyze the traffic patterns to deduce the location of the sink.

Due to the fact that traffic analysis is an effective mechanism to determine the geographic location of a sink, research concerning sink location anonymity in a sensor network has attracted a lot of attention. By hiding the sink node's true location, the cost to the adversary to locate the sink node increases.

Another important parameter in achieving sink node anonymity is the issue of node energy maintenance. Any anonymity scheme that is implemented in a WSN must ensure that the energy of the nodes is not significantly depleted; thus, a balance must be achieved in which sink node anonymity is attained while keeping node energy levels sufficient enough to continue network operations.

To address the issue of sink node anonymity, we develop a strategy to obfuscate the sink node's location using a hierarchical routing mechanism known as clustering while simultaneously limiting node energy depletion. To the best of our knowledge this is the first work that develops a novel sink node anonymity algorithm in a resource efficient manner. The contributions of this paper are summarized as follows:

- Development and implementation of a network topology and clustering algorithm in a resource-efficient manner.
- Development of a routing algorithm for sink node anonymity.
- Simulation and evaluation of the routing algorithm for security robustness and energy preservation.

The remainder of this paper is organized as follows. Section II provides an overview of the research in this area. Section III discusses the implementation of the clustering and routing algorithm along with a discussion of the anonymity factor. The results and analysis of the algorithm are given in Section IV. We conclude the paper in Section V.

## II. RELATED WORK

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 [4]. The layering architecture of a network facilitates the implementation of these subtasks. A network consists of 5 layers: physical, MAC, network, transport, and application. While there is research on specific attacks that target each layer, in this paper we are concerned with attacks at the network layer. There is abundant literature on anonymity at the network layer. Anonymity strategies implemented at the network layer require specific multi-hop routing protocols to be developed. There are a number of creative approaches to preserve WSN anonymity at the network layer. They can be divided into two types: source-location anonymity and sink-location anonymity approaches [3]. Because the focus of this paper is on sink node anonymity, we will discuss only those approaches that are relevant for this topic.

The challenge of location anonymity 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. One approach to deal with sink node anonymity is through the use of deceptive packets [5]. 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]. A disadvantage to the deceptive packet approach is that its performance is highly variable. 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.

Another approach to achieve sink node anonymity is through the  $k$ -anonymity algorithm, developed in [3]. 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 [3]. However, positioning  $k$  designated nodes within the WSN is complex as it affects two conflicting goals: the routing energy cost and the achievable anonymity level [3]. This is ultimately an optimization problem which requires prioritizing one goal or the other.

Another aspect of WSNs that has gained quite a bit of attention is energy conservation. This has resulted in the development of various approaches for saving the limited energy of the sensor nodes, thereby extending the life of the network [6], [7], [8], [9]. 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 [10].

Clustering is a hierarchical routing and topology management scheme commonly used in wireless networks. Low Energy Adaptive Clustering Hierarchy (LEACH) is a popular clustering based protocol that aims to minimize energy dissipation in sensor networks [11]. Sensor nodes form clusters and elect cluster heads (CH) which are then responsible for transmitting data to the sink node. Nodes within the cluster achieve energy savings by transmitting only to the CH. LEACH then rotates CHs to distribute energy requirements among all the sensors. Additionally, LEACH performs local computation at each CH (data aggregation) to reduce the amount of data that must be transmitted to the sink. This saves both energy and

bandwidth. There are a number of limitations to LEACH's practical application for current situations. LEACH assumes all nodes can transmit with enough power to reach the sink if needed, which limits its utility for a WSN deployed over a large area. In this sense, LEACH is not scalable for a broad number of applications. Also limiting the application of LEACH is that it was developed for sensing at a fixed rate and cannot support event driven or time sensitive reporting. The biggest limitation of LEACH stems from the fact that its primary focus of LEACH is of the network lifetime. It was not developed with security as a concern and has no features which address the security or privacy of data within a WSN. In the years since LEACH was published there has been additional research to address some of these limitations including E-LEACH, M-LEACH, LEACH-C and V-LEACH [12]. However, the solutions proposed in these LEACH extensions are not comprehensive.

### III. CLUSTER BASED ROUTING TO ACHIEVE ANONYMITY

In order to achieve energy constrained anonymity, we propose a routing algorithm based on node clustering which results in at least  $n$  other nodes having similar observable traffic statistics, thus obfuscating the sink nodes location. The steps that the WSN takes upon deployment to route traffic are as follows [13]:

- CH election and cluster formation.
- Choose a subset of the CHs to serve as broadcast CHs. The election of broadcast CHs, their importance in the network and the role they play in achieving sink node anonymity will be discussed in this section.
- CHs use Dijkstra's algorithm to determine their route to the sink nodes CH. Dijkstra's algorithm will be discussed later in this section.

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.

#### A. Cluster Head Election

Each sensor in the WSN may elect to become a CH with a fixed probability  $p$  when the network is deployed. There is not an optimal number of CHs for a WSN. For every topology the clustering process must ensure that no nodes become isolated and that there are no more clusters than necessary as excess clusters reduce the energy savings yielded from clustering. 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. We force this constraint on the sink node 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.

An iterative approach is utilized to balance the competing demands of preventing isolation and achieving energy efficiency. In this paper the probability of a sensor node electing to become a CH is fixed at  $p = 0.20$ . This value was experimentally determined so that most of the CHs are elected in the first iteration, while the additional two iterations serve to ensure that no sensor node is isolated in the WSN.

As stated earlier in this section, the sink node is never a CH; therefore, the sink node does not go through the process of electing to become a CH. The sink node simply looks for the nearest CH to join as a cluster member. The CH that serves the sink node is referred to as the sink node's CH.

1) *First Iteration:* In the first iteration, each node may elect to become a CH with a probability  $p$ . If a node does not become a CH, then it determines if there is a CH within transmission range. At the end of the first iteration, nodes belong to one of three categories: 1) node is a CH, 2) node is within range of a CH and 3) node is not a CH or within range of a CH.

2) *Second Iteration:* In the second iteration, all nodes that belong to category three at the end of the first iteration again elect to become a CH with probability  $p$ . All nodes which have not elected to become a CH in either iteration find the nearest CH within transmission range and elect to become a cluster member. If desired, the steps of the second iteration can be repeated as additional iterative steps. The benefit of additional iterations is that a lower initial  $p$  can be used. Using a lower  $p$  results in a more gradual election of additional CHs. With each iteration a few more CHs are elected until there is adequate connectivity coverage across the WSN. The more gradually CHs are elected, the more optimal the final number of CHs; however, there is an energy cost associated with executing each iteration. In this paper the total number of iterations is kept to three. We found that three iterations are sufficient to ensure that no nodes are isolated, and all nodes belong to a cluster.

3) *Final Iteration:* In the final iteration, any remaining nodes which are not in a cluster, that is not a CH or a cluster member, elect to become a CH.

#### B. Rotating the Cluster Heads in the WSN Topology

Clustering imposes a substantial energy burden on the nodes that act as CHs; therefore, it is necessary to rotate the role of CH within the WSN. We rotate the CHs for two reasons: load balancing and anonymity. The CHs are reelected in the same manner they were initially elected. The CHs are rotated when one of two conditions are met. Either one of the CHs has expended a certain amount of energy or a specific number of messages have been transmitted through the WSN. Implementing CH rotation allows us to distribute the burden of being the CH across the WSN while increasing the overall lifetime of the WSN. The CHs are rotated if 1) any CH

expends one percent of its initial energy value,  $\frac{E_o}{100}$ , where  $E_o$  denotes the initial node energy or 2) the sink node's CH receives 1000 messages. We set the energy threshold to one percent because the energy costs of routing traffic in the WSN are relatively low. We choose to rotate fairly often because we do not want the cluster topology of the WSN to be static for long periods of time. With a static topology it is plausible that the adversary could locate and inspect each node for which traffic is broadcast to in an effort to find the sink node [3]. Rotating the CHs increases the anonymity of the sink node by randomizing the paths that traffic takes through the WSN and makes it more difficult for an adversary to draw any conclusions as to the location of the sink node.

### C. Broadcast Cluster Head Election

The CHs in the WSN are responsible for routing data from the source nodes CH to the sink nodes CH. When forwarding data to the next node, each CH has two options. The message can be directly forwarded to the next node or widely broadcast to all sensors within range. In this algorithm we propose that a subset of CHs is selected to broadcast. One key consideration to broadcasting is overhead. We are aware that information is being transmitted to nodes that do not need it. In order to reduce overhead and limit broadcast information, we only allow a subset of CHs to broadcast to their members. The sink node's CH always broadcasts the messages it receives so that the sink node can receive the information. By broadcasting traffic to nodes other than the sink, we are essentially creating a situation where multiple nodes resemble the sink in terms of traffic volume. In other words, from the adversary's perspective, these multiple nodes are acting like sink nodes. In addition to the traffic volume, the cardinal direction of traffic is also disturbed. An attacker cannot use traffic volume for traffic direction to determine a sink node's location; thus, the cost of attacking each of these nodes is much higher than attacking just one (the sink node).

In choosing the broadcast CHs there are two key considerations: 1) The amount of residual energy remaining for the CH and 2) the number of cluster members of each cluster. The total number of broadcast cluster nodes is variable based on the number of members in each node. A lower threshold of 20 nodes broadcast to is established in this algorithm to ensure a minimum desired level of anonymity. The number of nodes broadcast to directly correlates to the anonymity of the sink node, as discussed later in this section (Section III-E) [13].

The CHs are ordered by their residual energy levels. The CH with the most energy is chosen to be the first broadcast CH. The number of cluster members which are broadcast to is then saved. Each subsequent broadcast CH is selected sequentially based on the most residual energy. The number of cluster members broadcast to is added to the previous value and, when the lower threshold for the number of nodes broadcast to (i.e., 20) is exceeded, no additional broadcast CHs are selected.

### D. Dijkstra's Routing Algorithm

Once broadcast CHs are determined, we must determine the paths that traffic takes to reach the sink nodes CH. Note that traffic should always be routed to the sink nodes CH, at which point the CH broadcasts data to the sink node and other cluster members. A source node with traffic to send always transmits to its CH. More specifically, communication paths are established between CHs and not individual sensor nodes. The path from source node to the sink nodes CH contains other CHs. Of those CHs, a subset broadcasts to their cluster members as well as the next hop CH.

To establish routing paths, we use Dijkstra's routing algorithm. Dijkstra's algorithm is a well-known, simple, least-cost algorithm that finds the lowest cost path from a source to a destination. Dijkstra's algorithm finds the shortest paths from a given source node to all other nodes by developing paths in order of increasing path length. Dijkstra's algorithm uses link costs to determine viable paths. Link costs are determined based on the network application. In this paper we use Euclidean distance as the cost between two CHs. The resulting path is the most energy efficient route through the WSN without factoring in the additional cost of the broadcast CHs. Due to space and the popularity of Dijkstra's algorithm, we refrain from discussing the algorithm here. We refer the reader to [4] for further details.

Fig. 1 shows an example of the final topology after clustering. The star represents the sink node, the red nodes represent the CHs and the blue nodes represent the subset of CHs that are chosen to be the broadcast CHs. The arrows indicate the paths for traffic routing using Dijkstra's algorithm.

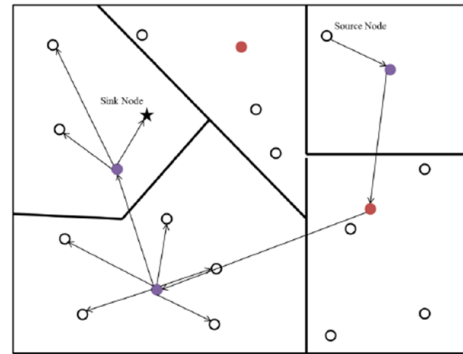


Fig. 1. All CHs use Dijkstra's algorithm to determine the least cost route to the sink node's CH. Broadcast CHs broadcast the data to all their cluster members.

### E. Sink Node Anonymity

The goal of developing this algorithm is to ensure that at least  $n$  other nodes in the WSN have similar traffic statistics as the sink node. Let  $N$  be the set of all nodes in the WSN and let  $i$  denote the total number of nodes. In this paper  $i = 100$  nodes: then,  $N = n_1, n_2, \dots, n_i$ .  $CH$  is the set of nodes

which serve as CHs. The total number of CHs is denoted as  $j$ :  $CH = ch_1, ch_2, \dots, ch_j$ .  $CM$  is the set of nodes which serve as cluster members. The total number of cluster members is denoted as  $k$ :  $CM = cm_1, cm_2, \dots, cm_k$ . At the end of the final iteration of the CH election, all nodes in the WSN are either CHs or cluster members.

$$N \equiv CH \cup CM \quad \text{and} \quad i = j + k \quad (1)$$

Each  $n_i$  in  $N$  becomes an element of  $CH$  or  $CM$ :

$$n_i = ch_b \in CH \quad \text{or} \quad n_i = cm_b \in CM \quad (2)$$

The set  $CH$  is then ordered by the residual energy within each node:

$$CH_{energy} = ch_5, ch_8, \dots, ch_j \quad (3)$$

$BBCH$  is the set of nodes which serve as broadcast CHs and is a subset of  $CH$ . The total number of broadcast CHs is denoted as  $m$ :

$$BCCH = bc_1, bc_2, \dots, bc_m \quad \text{and} \quad BBCH \subseteq CH \quad (4)$$

Each broadcast CH is selected in order of maximum energy remaining:  $bc_1 = ch_5$ ,  $bc_2 = ch_8$ , and so on. A broadcast CH broadcasts any data it receives to all of its cluster members in addition to the next hop CH. The total number of nodes broadcast to is denoted as  $\beta$ :

$$\beta = \sum_{i=1}^m \text{members}(bc_i) \quad (5)$$

The anonymity factor of the sink node is denoted as  $AF$  and is defined to be:

$$AF = \frac{1}{\beta} \quad (6)$$

The number of cluster members that belong to each broadcast CH change each time the CHs are rotated. To evaluate the anonymity factor, we take the average value of the cluster members broadcast to across the simulation:

$$AF_{topology} = \frac{1}{\text{average}(\beta)} \quad (7)$$

We use the preceding equations to evaluate the results of the simulations in Section IV.

#### IV. PERFORMANCE EVALUATION

##### A. Network and Threat Model

In our simulations, all the sensor nodes are placed inside a 100 meter x 100 meter square area. The locations of each sensor node is derived using pseudo random variables drawn from a standard uniform distribution on the open interval (0,1). These values represent the  $x$  and  $y$  coordinates of each node in meters in the WSN. The sink node is deliberately placed at the coordinate  $(x, y) = (25m, 75m)$ . While more than one sink node can be present in a WSN, in this paper we assume that only one sink node exists. We assume that each sensor has a fixed transmission range of 40m, allowing exchange of information with all nodes within that range. The sink node has the same fixed transmission range as the other nodes but

has more processing and power resources to handle traffic volume and relaying of information outside of the WSN. When the network is first deployed, all the nodes have the same initial energy levels. The energy of each node is depleted as the network is initialized (clustering process) and as traffic is routed. The transmit and receive communication costs are both fixed at  $5 \times 10^{-7}W$ . The processing cost is  $5 \times 10^{-8}W$ .

The sink node acts as a gateway between the multihop WSN and the wired infrastructure where the sensed information is analyzed. It is assumed that the wired network is not vulnerable to malicious traffic analysis. It is assumed that information is encrypted at the sensing node and is not decrypted until it reaches the sink node. It is assumed that the attacker has global knowledge of the traffic on the WSN and is involved in only passive attacks (i.e., only inferring location of objects and sinks using traffic analysis; the attacker is not interested in interfering with regular WSN communications).

All the simulations in this paper were performed on MATLAB. For the simulations, we generated four different physical topologies and conducted five trials using different traffic volume on each topology. A trial is defined as one set of traffic messages that are routed across a topology. The message traffic was generated in four different volumes: 5000, 10000, 15000, and 20000 messages. A different set of traffic was randomly generated in each trial.

##### B. Analysis and Discussion of Results

1) *Energy Efficiency Conclusions:* We first examined the average, minimum and maximum energy consumed by a node at each traffic volume on all four network topologies. The energy consumed includes energy used during the clustering process (as discussed in Section III) and from the traffic routing process using Dijkstra's algorithm.

The average energy consumed by a node at each traffic volume is plotted in Fig. 2. We see that the results are very similar to each other, with Topology 1 consistently less. We can expect variation among the topologies as the physical location of nodes (which are randomly distributed) will affect the energy consumption of each node in the WSN. The average energy consumed by a node increases as the traffic volume increases for each topology. For each topology we also examined the average minimum energy consumed by a node at each traffic volume. The results are shown in Fig. 3. The overall trend is that consumption increases with traffic volume across all four topologies. Similar to the average energy consumed, there is some variation among the results for the four topologies; however the results are very consistent, with no points being large outliers.

The maximum energy consumed by a node for each topology and traffic volume varies more than the average energy consumed and minimum energy consumed. These results are shown in Fig. 4. From Fig. 4, we see that the maximum energy consumed by a node are not as tightly grouped at any of the traffic volumes as they were in Fig. 2 and Fig. 3. The maximum energy consumed is harder to predict because

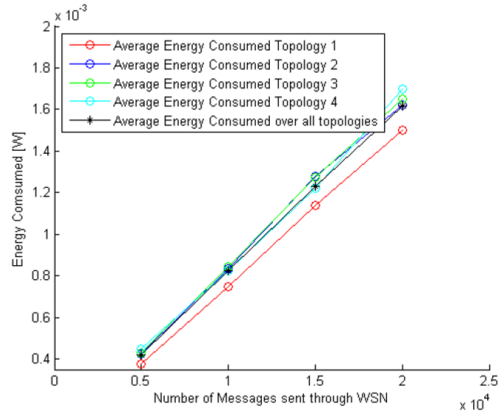


Fig. 2. Average energy consumed by a node for all four topologies and the average of the four

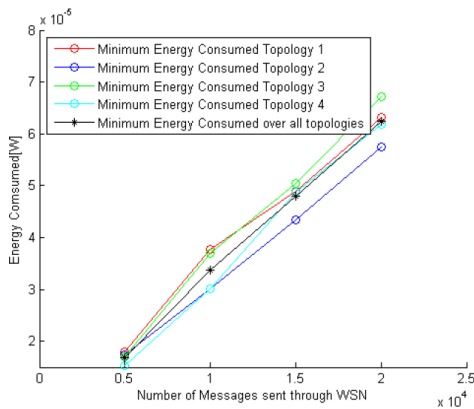


Fig. 3. Minimum energy values for all four topologies and their average

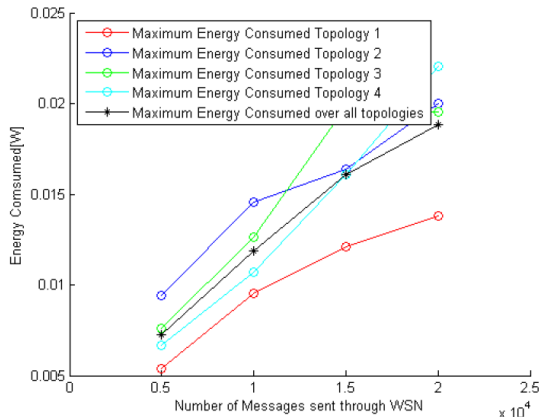


Fig. 4. Maximum energy values for all four topologies and their average

so many of the roles are chosen randomly, creating more variation.

Considering all four topologies individually and averaged together, we find remarkably consistent results for the average amount of energy consumed by a node in the WSN. This is promising because the average energy use by each node is an effective parameter for planning overall network lifetime. For simplicity, we did not let any nodes die out in these simulations because when nodes die the WSN may become partitioned, making the problem more difficult. Our goal was to evaluate the performance of the algorithm over a network where all of the nodes were alive.

2) *Sink Node Anonymity Conclusions:* The sink node anonymity was evaluated using Eqs. 6 and 7. From our simulations, we noticed that the number of nodes broadcast to was independent of the traffic volume; thus, we conclude that the overall anonymity factor of any WSN is also independent, as illustrated in Fig. 5. This is an important conclusion because, if the anonymity factor was reliant on a certain traffic volume, this would be a constraint for the employment of the algorithm and our objective is to have broad applications.

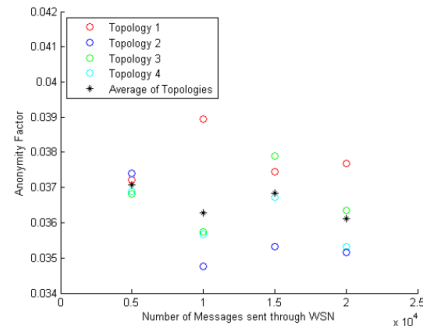


Fig. 5. The anonymity factor of each topology and the average anonymity factor calculated at each traffic volume

This conclusion leads us to examine the average number of nodes broadcast to at all message volumes to determine the anonymity factor for the topology. We see very consistent results across the four topologies, as illustrated in Fig. 6 and Fig. 7. We see variation between the four topologies, just as we did in the energy efficiency conclusions. We also see that the results are remarkably consistent. The value of the anonymity factor for each topology is under 0.04. This means that for any given topology we simulated an adversary conducting traffic analysis of the deployed WSN would have a less than 4% chance of finding the sink node on his/her first guess when physically searching for the sensor.

3) *Potential Algorithm Tradeoff:* The energy efficiency and anonymity metrics reflect that the proposed algorithm meets the desired result of being a privacy preserving algorithm approach and is also mindful of the of overall energy consumption and network lifetime.

However, the use of broadcast CHs generates extra network traffic. We found that approximately 20 additional nodes receive broadcast traffic when compared to only the sink node's CH broadcasting, regardless of the topology. The extra

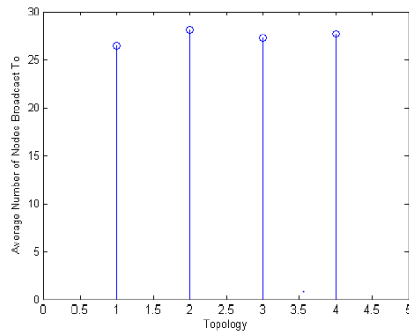


Fig. 6. The average number of nodes broadcast to for each topology, all traffic volumes included

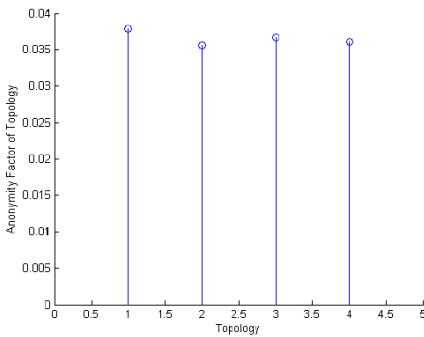


Fig. 7. The anonymity factor for all four topologies. The anonymity factor of all the topologies is calculated based on the average number of nodes broadcast to across all traffic volumes

traffic is necessary to achieve our desired level of anonymity, and the return on this extra traffic is significant with a more than 10% increase in the anonymity factor of the sink node as shown in Fig. 8; a higher anonymity factor means that there is a higher probability that the sink node will be found by the adversary. While the excess traffic can be considered a tradeoff for better anonymity, it should be noted that many of the schemes for anonymity preservation in a WSN introduced in Section II also have has significant overhead but do not achieve anonymity preservation and energy efficiency simultaneously.

## V. CONCLUSION

In this paper, we addressed the issue of sink node anonymity in a resource efficient manner. We developed and implemented a clustering algorithm in an energy efficient manner in conjunction with a routing algorithm that preserves sink node anonymity. We found that the anonymity factor of each network topology was independent of the traffic volume. We also found that the average energy consumed by a node was determined to be consistent across the four topologies in the simulations. This is promising because the average energy use by each node is an effective parameter for planning overall network lifetime. In our future work we intend to study how sink node anonymity is affected by the actual topology structure using graph theoretic models and also the impact of

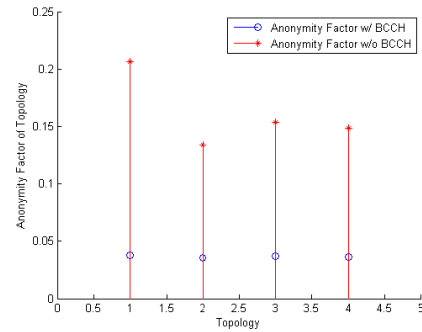


Fig. 8. The anonymity factor with the broadcast CH. The anonymity factor increases (which is a negative) without the use of broadcast CHs.

our algorithm when nodes begin to die out.

## REFERENCES

- [1] M. Conti, "Body, personal and local ad hoc wireless networks," in *The Handbook of Ad Hoc Wireless Networks*, M. Ilyas, Ed. CRC Press, 2003.
- [2] 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, pp. 320–336, February 2012.
- [3] G. Chai, M. Xu, W. Xu, and Z. Lin, "Enhancing sink-location privacy in wireless sensor networks through k-anonymity," *International Journal of Distributed Sensor Networks*, vol. 2012, pp. 1–16, 2012.
- [4] W. Stallings, *Data and Computer Communications*, Prentice Hall, 9 edition, 2011.
- [5] Y. Ebrahimi and M. Younis, "Using deceptive packets to increase base station anonymity in wireless sensor network," in *Proc. IEEE International Wireless Communications and Mobile Computing Conference*, 2011, pp. 842–847.
- [6] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, May 2009.
- [7] N. Perwaiz and M. Y. Javed, "A study on distributed diffusion and its variants," in *International Conference on Computing and Information Technology*, 2009, pp. 44–49.
- [8] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. ACM International Conference on Mobile Computing and Networking*, 2000, pp. 56–67.
- [9] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," *Wireless Networks*, vol. 8, no. 2, pp. 169–185, March 2002.
- [10] 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*, 2010, pp. 1–6.
- [11] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. IEEE Annual Hawaii International Conference on System Sciences*, 2000, pp. 1–10.
- [12] A. Rahman, "A survey on energy efficient routing techniques in wireless sensor network," in *International Conference on Advanced Communications Technology*, 2013, pp. 200–205.
- [13] A.F. Callanan, "Achieving sink node anonymity under energy constraints in wireless sensor networks," M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, June 2014.