Journal of Scientific Research and Development 2 (7): 171-177, 2015
Available online at www.jsrad.org
ISSN 1115-7569

Improving the security and reliability of wireless sensor networks based on an effective algorithm for boosting base station anonymity

Ali Barati *, Iman Attarzadeh

Department of Computer Engineering, Faculty of Engineering, Islamic Azad University, Dezful Branch, Dezful, Khouzestan, Iran

Abstract: Wireless sensor networks (WSNs) have shown great potential for serving a full spectrum of applications in a wide variety of environments. Of special interests are applications that operate in hostile setups such as combat zones and territorial border. These applications are categorized with the presence of adversaries who are eager to attack the network. The most effective approach for an adversary to do so is by targeting the Base-Station (BS), where the sensor data are collected in the field. By identifying and locating the BS, the adversary can launch attacks to damage or disrupt the operation of the BS. Therefore, sustaining the BS anonymity is of highest importance in WSNs. This research aims to propose an effective algorithm for boosting base station nodes anonymity to protect them from potential threats. In the first step, the distribution of more base station nodes is conducted to analyze and compare the base station anonymity of a node versus multiple base station nodes under different network topologies. In the second step, the mobility of base-stations and the effect of relocating some of the existing BS nodes to the lowest anonymity regions are conducted and analyzed. The obtained results show that using more base stations can increase the average anonymity of base station nodes; also using one mobile base station can increase the anonymity of the WSN.

Key words: Wireless sensor networks; Anonymity; Traffic analysis; Network architecture; Dynamic association; Network clustering

1. Introduction

A Wireless sensor network is typically composed of a large set of miniaturized sensor nodes that report their findings to a nearby base-station (BS). The BS tasks the sensor nodes, processes the data, and interfaces the network to remote users. The important role that the BS plays makes it a critical asset for the network and would thus become a primary target of adversary's attacks. The adversary will focus all efforts on uncovering the identity and location of the BS in order to launch attacks to disrupt or damage the BS. In fact, given the unattended network operation, the adversary can even capture the BS and extract stored sensitive information, or replace the BS with a malicious one. Therefore, keeping the BS's identity and location anonymous is of utmost importance in WSNs. Since, the sensors nodes are battery-operated and have a limited lifespan, multi-hop routes are usually pursued to disseminate the collected data to the BS (Akyildiz et al., 2012; Chong and Kumar, 2013). As the BS serves as the sink of all data traffic, an adversary would try to determine the routing topology to identify the BS. Contemporary anonymous routing techniques (Seys and Preneel, 2014; Zhang et al., 2009; Boukerche et al., 2014) cipher the packet header in order to conceal the ID of the BS so that the adversary cannot extract it from an intercepted packet. However, anonymous routing does not suffice since the adversary can still pursue link layer based analysis. Basically, the adversary would intercept RF transmission, localize the source and determine the range. By correlating the intercepted transmissions both spatially and temporally the adversary can detect links between nodes and aggregate them to form data paths. Such terrific analysis can uncover the position of the BS and make the network vulnerable.

A number of techniques have been proposed in the literature for boosting the BS's anonymity. Most of these techniques focus on concealing BS's role by spreading the network traffic to disguise the role of BS as a sink (Deng et al., 2012; Conner et al., 2009) preventing hop-to-hop packet tracing (Ebrahimi and Younis, 2013), and relocating the BS (Acharya and Younis, 2012). However, all the techniques have assumed network architectures with a single BS node. Few studies have been conducted for networks with multiple BS nodes and assessed their impact on anonymity. In additional, although relocating the BS to a safer spot has been pursued, few prior works have exploited the possibility that a mixture of mobile and stationary BS nodes are deployed and tried to take advantage of that in boosting the anonymity. This research tries to fill this gap and study the impact of the number and mobility of the BS nodes on anonymity. The goal is to provide guidelines for the network designers in order to determine the appropriate resources and node

* Corresponding Author.

capabilities and conduct trade-off between anonymity and other metrics like cost.

2. Related work

Security and reliability in Wireless Sensor Networks (WSNs) has been intensively researched in the literature. WSNs require most of the common security requirements of typical networks and also pose unique characteristics which need to be addressed in a non-conventional way.

2.1. Data confidentiality and integrity

Data confidentiality and integrity are usually the top security priorities in any distributed systems, WSNs are no exception since it is common for WSNs to be deployed to serve mission critical applications, and the data collected by each node and aggregated information can be highly sensitive. To protect the data of WSNs from eavesdropping and manipulation at data link and network layer, lightweight encryption is pursued (Youssef et al., 2010). Key management and key distribution (Li et al., 2009; Yang, 2007) are very critical to the security of WSNs since strong encryption is the first layer of defenses. Because of the limitation of computational power and physical energy, most of the traditional asymmetric public key management/distribution schemes are not directly applicable to WSNs since they are very computational extensive and do not assume a network with thousands of participating nodes. One of the significant studies on WSN key management/distribution is published Du et al. (Du et al, 2008). In the research, the authors have proposed an effective and lightweight approach to tackle the problem of constrained memory of sensor nodes. They utilize a random key pre-distribution schema that exploits deployment knowledge. With such knowledge, each sensor only needs to be assigned the relevant keys which are necessary for it to communicate with its neighbor or base stations, therefore avoiding unnecessary key assignments.

2.2. Network anonymity and traffic analysis

Even if the confidentiality and data integrity measures are perfectly implemented, adversaries still can deduce valuable information by analyzing the network traffic without knowing the contents of data packets. Protecting the Base station (BS) is the utmost task in countering traffic analysis attacks because of the special role it plays in WSNs. As a data collector, data gathered by the low energy sensor nodes will be eventually routed to the BS nodes, and uneven network traffic will be created around them. Therefore, one of the major issues is how to balance the network traffic throughout the network and also hide the fact that data packets are converging to the BS. Deng et al. (Deng et al., 2012) introduced a set of algorithms to defend against traffic analysis. First, they proposed a multi-parent scheme, where each sensor has multiple parents on the routing tree and randomly chooses a parent to forward packets. The second technique introduced is called random walk. In both of these techniques randomness is introduced in the data forwarding path to the BS. The third technique is called fake path, where redundant packets are injected into the network in order to mislead the adversary into believing that the BS at the destination of the redundant packets. Conner et al. (Conner et al., 2009) proposed to use data aggregators to disguise the real location of the BS. Aggregators are called decoy sinks with data packets forwarded to them, and then they process and aggregate the sensor readings before sending to the BS. The major problem with this approach is that a decoy sink under this assumption is a de-facto BS. If adversary takes out the decoy sink, the network operation will be disrupted as well. Acharya and Younis (Acharya and Younis, 2012) proposed the BAR approach. The idea is simply to make the BS disguises itself by transmitting BAR packets with varying intensity to its neighbor when it receives data packets. The possibility of re-transmitting BAR packet diminishes each time the BAR packet is forwarded. BAR packets can be forwarded away to a region far away from the BS and mislead the adversary into believing that the BS is just an intermediate sensor. The BS relocation is also studied in (Acharya and Younis, 2012). A relocation technique is introduced in order to safeguard BS while moving. Meanwhile, the approach of (Ebrahimi and Younis, 2013), changes the transmission power of the individual sensors in order to increase the node degree and complicate the traffic analysis and slow its convergence. Although the above mentioned approaches have helped increasing the anonymity of the BS to some extent, they all have made the assumption that there exists only one BS. While multiple BS nodes have been studied extensively under other metrics like data latency and energy conservation (Savvides et al., 2006; Niculescu and Nath, 2011), no study has accessed the impact of multiple BS nodes on anonymity. Also, few studies have tried to use a mixture of mobile and stationary BS nodes to boost BS anonymity.

2.3. Sensor clustering

Grouping nodes into clusters has been pursued by many researchers as a means for efficient network management. Clustering in WSNs is significantly different from traditional clustering mechanism in general ad-hoc networks. In a typical network, the clustering objective is to generate stable route among mobile nodes, whereas in WSN, sensor clustering opts to achieve better scalability and network longevity. Clustering algorithms in WSNs usually elect a cluster head (CH) to manage the sensors within the group. Published approaches vary in the way they choose a CH, and in the criteria of assigning sensors to a cluster. A CH can be either statically appointed, or elected among the peer sensors, or based on a predefined round robin

schedule (Xu et al., 2011; Adamou et al., 2001). Different layers of clustering can be utilized to build a hierarchical network (Bandyopadhyay and Coyle, 2003; Banerjee and Khuller, 2010) and the sensors' membership in a cluster can be fixed or variable. In WSNs with multiple BS nodes, it is typical to designate the powerful BS as a CH rather than a sensor. If sensor nodes are not uniformly distributed around the BS nodes the clusters formed will have different load, which will affect the lifetime and energy consumption of the system. (Younis et al., 2006) introduced an approach to cluster unattended wireless sensors while balancing the load among the clusters in order to increase the node lifetime and lower processing delay. In this research, dynamic association of sensor to clusters is exploited, so that the traffic pattern changes and the traffic intensity is equalized in the various clusters and consequently the adversary will have hard time correlating the transmissions and determining the data paths.

3. Research method

3.1. System model

In this research, the most typical WSN model is considered. All the sensor nodes have limited but similar capabilities including energy, communication range, and link bandwidth. Besides sensor nodes, there will be one or multiple BS in the WSN. The BS nodes are of two types: stationary and mobile. A mobile BS is able to move within the WSN area as needed. The BS serves as data sink of all data traffic originated at the sensors. In the presence of multiple base-stations, each sensor node picks the closest BS to send the data packets to. It is assumed that sensors know their positions relative to the BS nodes by applying localization algorithm such as (Youssef et al., 2010). Least-cost multi-hop routes are pursued for disseminating data packet to the BS with communication energy used as the link cost. In addition, it is assumed that an anonymous routing protocol such as (Seys and Preneel, 2014) is employed in order to conceal the identity of the BS nodes while ensuring the data integrity and authenticity of the source of packets. The Wireless Sensor Network is assumed to be serving target detection and tracking application in an inhospitable environment. It means when a target of interest enters the detection range of a sensor node, the sensor will be immediately noticed and such finding is reported back to BS nodes via the multi-hop communication. Besides that, there is no periodical communication between sensor nodes and BS nodes.

The adversary may use signal detection techniques such as angle of arrival, received signal strength, etc. (Li et al., 2009; Yang, 2007) and then apply localization algorithms (Du et al., 2008; Savvides et al., 2006) in order to determine the position of the individual nodes. The adversary then performs correlation of the intercepted transmissions to identify active communication links and the data paths. To facilitate the traffic analysis, the adversary divides the entire area into a number of equal-size cells. The size of a cell reflects the accuracy of the localization of the source of the RF transmission. Based on the transmission power, the adversary determines the neighboring cells that potentially host the recipient. In other words, the traffic analysis is performed on the level of cells with the goal of finding out the cell that has the BS. The adversary is mobile and can move from one physical location to another. Upon identifying the BS cell, the adversary conducts an exhaustive search and may use careful and thorough visual inspection to recognize the BS. While the adversary can intercept packets, it is assumed that the cryptosystem is so robust that the adversary cannot apply cryptanalysis to decrypt the contents of the packets. The adversary is also assumed to be a passive listener and does not inject its own packet into the network. Next subsection first explains the metric used for assessing the BS anonymity and then describes the proposed approaches for increasing the BS anonymity in WSNs.

3.2. Anonymity Evaluation

In order to quantity the BS anonymity, the modified version of GSAT test proposed in (Acharya and Younis, 2012) is employed. The GSAT test is first proposed by Deng et al. (Deng et al., 2012) as a tool for measuring the average number of steps an adversary makes until finding the cell where the BS is located. The idea is to proceed in a greedy manner by identifying radio transmission/reception hotspots and gradually move to the area where the BS is stationed. The adversary starts from a random cell and monitors radio communication within its vicinity, which includes its own cell and all the adjacent cells. After a certain period of time, the adversary counts the radio activities that were intercepted and moves to the neighboring cell with the highest transmission count. If the adversary's cell experiences the most activities, the search for the BS is said to be stuck at a local maxima. The greedy search terminates if the BS cell is reached, and the corresponding number of moves that the adversary takes is said to be the GSAT number. However, given the assumed adversary capabilities, the adversary will not be able to visually identify the BS even if it is in the same cell, the GSAT test will never terminate unless the adversary pauses for long time every time a local maximum is encountered. In the modified version of GSAT (Acharya and Younis, 2012), the total number of moves taken and the number of times the adversary visits the individual cells are tracked. At any given time t, the GSAT score of a cell i is defined as:

$$G(i,t) = \frac{no\_of\_cell\_visits}{\text{no\_of\_total\_moves}} \quad (1)$$

GSAT scores of all the cells at any time t should sum up to 1, i.e. $\sum_{i}^{n} G(i,t) = 1$, where n is the total number of cells. GSAT score is a very helpful

indicator for whether a cell hosts the BS. Since all data packets must ultimately be forwarded to BS, it is inevitable to have the BS cells as radio activity hotspots. This uneven traffic pattern especially helps the adversary assess the likelihood that a cell hosts the BS. GSAT score captures the essence of WSN traffic pattern: if an adversary visits one particular cell again and again due to its high activities count, it can be concluded with high confidence that the BS resides in that cell.

3.3. The proposed algorithm

The sensor dynamic re-association (DR) scheme proposed below is a novel approach to introduce irregularity in the traffic and balance the inward traffic to the individual BS nodes in order to nullify adversary's effort on traffic analysis without creating completely different network architecture using mobile nodes. The DR algorithm will only be performed by source nodes to avoid unnecessary calculation and communication overhead on the other sensors in the network. Another traffic pattern can easily observe is that if a target is moving slowly or stays still in the WSN, a continuous stream of data packets will be flowing into the BS nodes which the source nodes report to. Therefore, the anonymity of those BS nodes will diminish and they become gradually exposed to the adversary. The proposed algorithm uses a rotation scheme to disperse the outgoing data packets of source nodes into different receiving BS based on proximity.

After WSN starts, each sensor node calculates the distances to every BS nodes in the field, and stores the BS nodes' ID in increasing order according to their proximity. The default BS to report to is the first BS in the list, also the closest BS. Whenever a sensor detects a target in its vicinity and becomes a source node, it will check with its current associated BS whether the BS is safe. Upon receiving such inquiry, the BS will examine its anonymity level based on Max GSAT score. If the GSAT score is higher or lower than a safety threshold, BS will tell the source node that sent the inquiry to re-associate to another BS, or keep sending data packets. If sensor re-association is recommended, the source will simply change the current BS to the next BS in the candidate list, and all the subsequent data packets will be forwarded to the new BS. When the current BS is the last entry (furthest BS) in the candidate list, the source node will re-associate with the first BS (closest BS) in the list.

To avoid unnecessary operation, the proposed algorithm will only be called if the WSN is in an unsafe state. The pseudo code of the proposed dynamic sensor re-association is described in Fig. 1. Part A demonstrates the establishment of candidate list for every sensor after the network bootstrapping. Part B describes the detailed implementation of a source node re-association. Note that the variable anonymity_threshold is the safety threshold and it is set to be 1.5 times the Average GSAT of all the cells. That means, in a 10-cells topology the anonymity_threshold is 1/10 * 1.5 = 0.15 and a BS considers itself to be safe if it has GSAT score lower than 0.15.

```
Part A: When network starts:
1. For sensor = 1 to N_Sensor
2. Sort (sensor–> BS_Candidacy)
3. End For

Part B: While network is in operation, loop indefinitely:
1. If MAX_GSAT > anonymity_threshold
2.  For sensor = 1 to N_Sensor
3.   If sensor = source_node
4.    //check current BS's GSAT value
5.    gsat = GSAT(BS_Candidacy(current_BS))
6.    If (gsat > anonymity_threshold)
7.     //change BS only if no recent BS changes were
made
8.      If curr_time - sensor –> last_move > t_interval
9.       current_BS = (current_BS + 1) % N_BS
10.      Sensor –> last_move = current_time
11.    End If
12.   End If
13. End If
14. End For
15. End If
```

Fig. 1: Dynamic Re-association (DR) Pseudo Code

4. Experiments, results, and discussion

4.1. Simulation setup

A simulation environment in JAVA developed for a WSN serving target tracking applications. A screenshot of the simulation application is shown in Fig. 2. In the simulation experiments, a set of sensor nodes is uniformly spread over an area of 1000 × 1000 meters to monitor targets crossing the area. The distribution of the M BS in the area follows a uniform random distribution with the restriction that no more than one BS can reside in the same cell. This constraint is also observed when relocating a BS. The restricted BS placement is important in order to prevent multiple mobile BS nodes from moving into one cell and creating a de facto one BS setup. In the simulation, BS movement takes place instantaneously and the travel path, delay and overhead is not factored in the results.

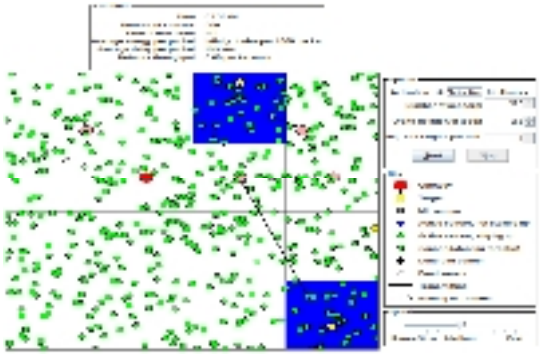

Fig. 2: Screenshot of the Java Wireless Sensor Networks Simulator

The number of targets in the simulation area at any simulation time is in the range of 1 to 4. The

targets move randomly within the simulation area. When a sensor node detects a target within its range, it reports such a finding to the closest BS over the least cost multi-hop path. The link cost in the experiment is taken to be the communication energy. In the experiments sensors have radio communication range of 200 meters, and tracking range of 100 meters. Although in reality the BS is capable of transmitting packets to a much further range, set its communication range to be 200 meters because the BS wants adversary to believe that it is just another sensor. Three grid configurations are considered in the experiments, namely, 16 cells of 250 ×250 meters, 25 cells of 200 × 200 meters and 64 cells of 125 x 125 meters. In practice, the cell size is determined by the adversary based on the signal interception capabilities. These three cell sizes configurations used in order to study the impact of the cell size selection on anonymity. The GSAT score is used as metric for measuring anonymity. The sampling interval used by adversary in the simulation is 10 minutes, which means the adversary monitors traffic in its vicinity for 10 minutes before making decision where to move to. To study the effect of node density on performance, two sensor counts, 100 and 500, have used to make the average node degree to be 12.56 and 62.83, respectively. The node density will affect the complexity and convergence of the traffic analysis. For each simulation experiments with M BS, have made tested with 0, 1, 2 ... M of the BS nodes being mobile. The results of the individual experiments are averaged over 30 runs. All results are subjected to 90% confidence interval analysis and stay within 10% of the sample mean.

4.2. Analysis of effect of BS count

The Average GSAT score for 25 Cells and 500 Sensors under varying number of BS count is shown in Fig. 3. As expected, using multiple BS increases the anonymity (decreases the GSAT score). A drop of 50% in the average GSAT scores is observed when deploying 2 BS nodes rather than one. The drop rate is not sustained though when employing more than 2 BS nodes. The GSAT scores of 1 BS's scores drop by only 73.2% when 6 BS nodes are used. It is worth noting that the result is also sustained over time.

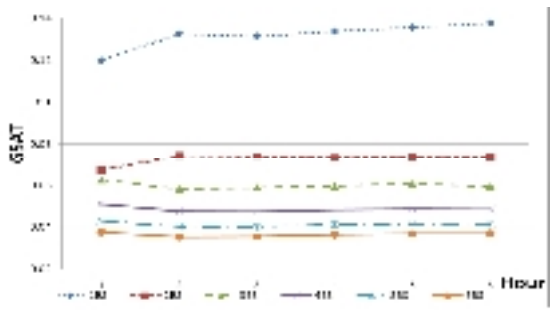

Fig. 3: Average GSAT of BS in 25 Cells, 500 Sensors with all stationary BS nodes

4.3. Analysis of effect of BS mobility

In this subsection, to ease data comparison with BS setup with all stationary BS, all the results are generated using 25 Cells, 500 Sensors setup. The average GSAT is shown in Fig. 4. Compared to Fig. 3, the Average GSAT scores Fig. 4 drop sharply after making only one of the BS mobile. For example, allowing 1 mobile BS in 3BS setup reduces the average GSAT from 0.059 to 0.033 at hour 6, which is about 44.1% drop. In extreme cases like 1BS (1 Mobile), where the only BS in the WSN is mobile, the average score is nearly 0 for the entire simulation time. The result proves that the mobile BS can keep a very low anonymity status by relocating to the lowest GSAT cell. If the network traffic is redirected to the new cell, mobile BS can move again to avoid detection by the adversary.

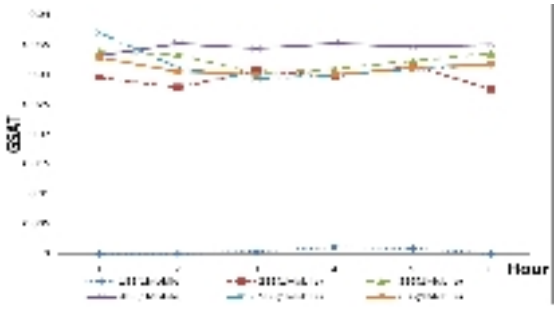

Fig. 4: Average GSAT of BS in 25 Cells, 500 Sensors with 1 mobile BS node

The next scenario to explore is the impact of anonymity if all BS in the WSN are mobile. The results of all mobile BS are shown in Fig. 5. Compared to results in Fig. 4, all-mobile BS setups boost the anonymity of BS even further in every BS count. For example, at Hour 5, the average score for 5BS (5Mobile) is 0.012 in Fig. 5, while average score for 5BS (1Mobile) is 0.03 in Fig. 4, which is higher than a factor of 2.5. When the BS grows, such a race condition become more likely to happen, which explains why topologies with high BS count are actually less secure if all BS nodes are mobile. A coordinated relocation of BS nodes can be an effective means for overcoming this issue.

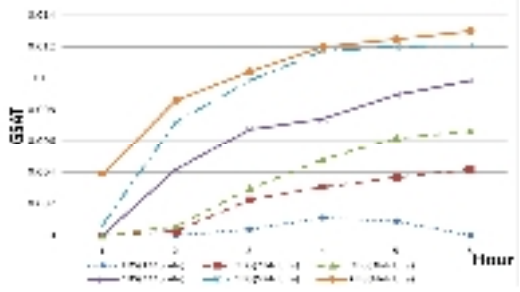

Fig. 5: Average GSAT of BS in 25 Cells, 500 Sensors with all mobile BS nodes

In addition, the ratio of the mobile BS count to the total BS count matters on anonymity. For example, in a 50% mobility setup, e.g., 2BS (1Mobile), has higher GSAT scores than the corresponding 100% mobility

setup, i.e., 2BS (2Mobile). Table 1 shows the observed effect of mobility ratio on anonymity.

Table 1: Average GSAT of BS after 6 hours with different percentages of BS mobile in 25 Cells, 500 Sensors

0%		
33.3%		
66.7%		
100%		

4.4. Effect of dynamic Sensor re-association

In the simulation process all the sensor nodes employ the algorithm discussed in earlier section to make on-the-fly decision about which BS to report to, based on the current GSAT value of BS nodes. The DR algorithm is especially useful when the target is moving slowly. To analyze the effect of target speed on performance of the algorithm, 3 different sets of speeds have used for the target: 0.05, 0.1, and 0.5 meter/second. The Average GSAT of BS with and without using DR along 6 hours of simulation time is shown in Fig. 6.

As expected, the proposed DR algorithm successfully decreases the Average GSAT value for all three speeds. For example, when the speed is 0.5, the Average GSAT without using DR is 0.063 at hour 4, while the DR's result is 0.056, about 11 percent lower. When speed is 0.1, DR drops the Average GSAT from 0.059 to 0.053 at hour 5, also about 10 percent less. From the same Fig., can also notice a clear pattern that a slower target speed will lead to higher average GSAT. Without implementing DR, at hour 4, speed 0.5 and speed 0.05 have Average GSAT value 0.062 and 0.047, respectively, which constitutes a 25% gap. This confirmed the expectation that a slow-moving or stationary target will generate more unbalanced network traffic since the same set of source nodes will periodically reports to the same BS nodes.

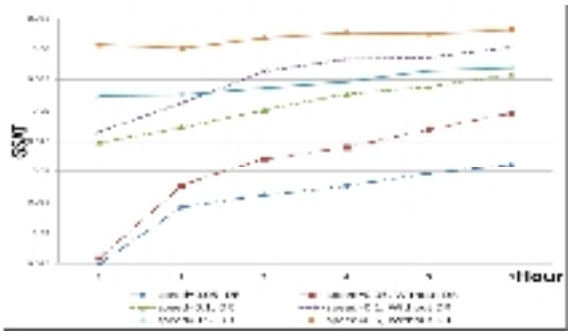

Fig. 6: Average GSAT of BS in 4BS, 25 Cells, 500 Sensors with or without Dynamic Re-association

Fig. 7 summaries the effect of target movement speed on the percentage of GSAT change at Hour 5.When the target speed is 0.05, the Average GSAT drops 15.5% with DR compare to not using DR. When the target speed is doubled to 0.1, the Average GSAT is only decreased by 8.1% by DR. The level of changes is maintained at 7.9%, even though the speed is further increased to 0.5.

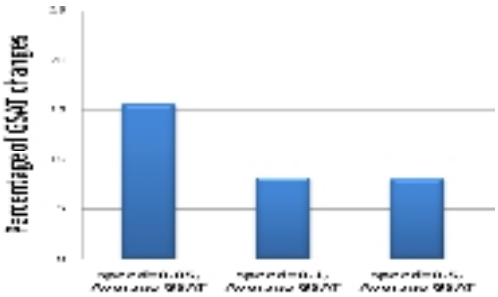

Fig. 7: Effect of Target movement speed on percentage of GSAT changes at Hour 5 in 4BS, 25 Cell, and 500 Sensors

5. Conclusion

Many WSN applications serve in hostile environments, such as combat field reconnaissance, border protection, and security surveillance, where the network may be subject to adversary's attacks. Given the role that the base-station (BS) plays, it is the most attractive target for an adversary who opts to inflict maximum damage to the operation of the WSN. The fact that the BS is the sink of all data traffic makes it vulnerable. Even if packet encryption is pursued, an adversary can intercept the individual wireless transmission and employ traffic analysis techniques to follow the data paths. Since all active routes ends at the BS, the adversary may be able to determine its location and launch targeted attacks. Therefore, countermeasure must be employed to boost the BS anonymity and avert adversary's attacks.

This research has proposed the approaches to counter traffic analysis and increase the anonymity level of BS nodes. First, the effect of the BS multiplicity and mobility on anonymity analyzed. Through simulation, it has been shown that the increased BS count always have a positive effect on anonymity since it spread the traffic and prevent the formation of a hotspots in the vicinity of base-stations. In addition, the BS mobility proved to be an effective means for increasing anonymity. However, having multiple mobile BS nodes may not be an asset to the network since they may decide to do the same spot and cause a hotspot. Coordinated BS motion is recommended and is part of the future work plan. In WSNs where mobile BS nodes is not applicable, sensor dynamic re-association have introduced to disperse the emerging traffic on some particular BS node and achieved better load balancing among all BS nodes.

References

A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "A Novel Solution for Achieving Anonymity in Wireless Ad hoc Networks," Proceedings of the 1st ACM international workshop on Performance

evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN' 2010), Venice, Italy, pp. 123-138, July 2014.

A. Savvides, C. Han, M. Srivastava, "Dynamic Fine-grained Localization in Ad-hoc Networks of Sensors," Proceedings of the 7th Annual International ACM Conference on Mobile Computing and Networking (MobiCom'06), Rome, Italy, pp. 267-279, July 2006.

A. Youssef, A. Agrawala and M. Younis, "Accurate Anchor-Free Localization in Wireless Sensor Networks," Proceedings of the 1st IEEE Workshop on Information Assurance in Wireless Sensor Networks (WSNIA 2010), Phoenix, Arizona, 45-56, April 2010.

CY. Chong, S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," Proceedings of the IEEE Networks, Vol. 91, No. 8, pp. 1247- 1256, August 2013.

D. Niculescu, B. Nath, "Ad hoc Positioning System (APS) Using AoA," Proceedings of IEEE INFOCOM, San Francisco, CA, pp. 227-236, April 2011.

F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E Cayirci, "Wireless sensor networks: a survey," Computer Networks, Vol. 38, No. 4, pp. 393-422, March 2012.

J. Deng, R. Han, and, S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," Proceedings of the 1st International Conference on Security and Privacy For Emerging Areas in Communications Networks, pp. 14-26, September 2012.

M. Adamou, I. Lee, I. Shin, "An energy efficient real-time medium access control protocol for wireless ad-hoc networks," Proceedings of WIP Session of IEEE Real-time Systems Symposium (RTSS'01), London, UK, pp. 207-218, December 2001.

M. Younis, P. Munshi, G. Gupta and S. Elsharkawy, "On Efficient Clustering of Wireless Sensor Networks," Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006), Columbia, Maryland, pp. 32-47 , April 2006.

S. Bandyopadhyay, E. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03), San Francisco, California, pp. 57-62, April 2003.

S. Banerjee, S. Khuller, "A clustering scheme for hierarchical control in multi-hop wireless networks," Proceedings of 20th Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'10), Anchorage, AK, pp. 347-359, April 2010.

S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications, Vienna, Austria, pp. 65-78, April 2014.

U. Acharya and M. Younis, "Increasing Base-Station Anonymity in Wireless Sensor Networks," Journal of Ad-hoc Network, Vol. 8, No. 8, pp. 791-809, November 2012.

W. Conner, T. Abdelzaher, K. Nahrstedt, "Using Data Aggregation to Prevent Traffic Analysis in Wireless Sensor Networks," Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS'09), Springer-Verlag, LNCS 4026, pp. 235-248 June 2009.

W. Du, J. Deng, Y. Han, S. Chen, P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge,"Proceedings of 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'08), pp. 197-213, March 2008.

X. Li, H. Shi, Y. Shang, "A Sorted RSSI Quantization based Algorithm for Sensor Network Localization," Proceedings the 11th International Conference on Parallel and Distributed Systems (ICPADS' 09), Fukuoka, Japan, pp. 98-107, July 2009.

Y. Ebrahimi, and M. Younis, "Increasing Transmission Power for Higher Base-station Anonymity in Wireless Sensor Network," Proceedings of the IEEE International Conference on Communications (ICC 2013), Kyoto, Japan, pp. 186-197, June 2013.

Y. Xu, J. Heidemann, D. Estrin, "Geography-informed energy conservation for ad hoc routing," Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'11), Rome, Italy, pp. 76-89, July 2011.

Y. Yang, "Target Source Detection using an Improved Sensing Model in Wireless Sensor Networks (ISMWSNs)," Proceedings of the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'07), Lyon, France, pp. 345-358, August 2007.

Y. Zhang, W. Liu, and W. Lou. "Anonymous Communications in Mobile Ad hoc Networks," Proceedings of IEEE Information Communications Conference (INFOCOM), pp. 138–146, March 2009.