

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A. A. Elkhail, U. Baroudi and M. Younis, "WSN Routing Protocols: Anonymity Prospective Analysis," *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, Al-Khobar, Saudi Arabia, 2022, pp. 819-823, doi: 10.1109/CICN56167.2022.10008348.

<https://doi.org/10.1109/CICN56167.2022.10008348>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

WSN Routing Protocols: Anonymity Prospective Analysis

Abdulrahman Abu Elkhail and Uthman Baroudi

*Department of Computer Engineering
King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia
g201536490,ubaroudi@kfupm.edu.sa*

Mohammed Younis

*Department of Computer Science and Electrical Engineering
University of Maryland Baltimore County
Baltimore, MD 21250, USA
younis@cs.umbc.edu*

Abstract—A Wireless Sensor Network (WSN) is mainly composed of multiple sensor nodes and a single Base-Station (BS), randomly distributed in a given area of interest. WSNs have proven very beneficial in various applications in unattended setup in many domains such as scientific, civil, and military. In these applications, sensors send their measurements to the Base Station over multi-hop wireless routes where the Base Station is responsible for collecting and processing the sensed data. Given the significant role of the BS, an adversary would try to uncover the base-station position by analyzing the traffic patterns in the network in order to apply targeted attacks that are geared for disrupting the network operation. In this paper, we analyze the traffic analysis attack models from an adversary's point of view. Also, we evaluate different routing schemes in order to assess the strengths and weaknesses in terms of exposing the network to traffic analysis attacks. Our evaluation is supported by simulation results.

Index Terms—Traffic Analysis, Wireless Sensor Networks, Location privacy, routing protocols.

I. INTRODUCTION

Wireless Sensor Network's (WSN) show incredible potential towards serving a lot of applications that generally work in harsh environments like combat fields reconnaissance, transportation, border protection, military and security surveillance [1]. A WSN typically consists of multiple sensor nodes and a single Base Station (BS), which are randomly distributed in a large deployment area. The sensor nodes are utilized to monitor environmental conditions like temperature, humidity, pressure, lighting condition, to name a few. These measurements follow a fixed path charted from sensor nodes towards the BS over wireless links. The sensor nodes typically use the shortest path (SP) routing scheme to disseminate their data to the BS which makes the nodes close to the BS forward an altogether more prominent volume of packets than nodes further away from the BS [2]. This produces very articulated traffic designs that uncover the bearing towards and thus the area of the BS.

In addition to receiving and processing the collected measurements, the BS tasks the sensor nodes, and interfaces the network to remote users. The BS thus becomes a basic

necessity for the network to function and subsequently turns into a target for the adversary's attack. The adversary plays a major role in revealing the identity and location of the BS so as to dispatch attacks to disturb or damage the BS. Indeed, given the unattended network activity, the adversary can even catch the BS and extract stored sensitive data, or replace the BS with a malicious one. In this way, keeping the BS's identity and location unknown is very important for WSNs. The adversary's main purpose is to protect the base station from the WSN's values which could potentially harm the base station and it does it by avoiding to deal with individual sensor nodes. Anonymity refers to the state of being indistinguishable. In the realm of WSN, anonymity can be characterized as concealing an identity, role and location of the base station from external observers. At the node design level, the BS could be camouflaged to blend in the surrounding objects. Yet, tracking data transmissions could allow detection. In usual cases, packet encryption and anonymous routing are often used to disguise the base station's identity [3] and adversary's utilize the traffic analysis techniques to locate the base station. [4], [5]. Adversaries can always determine the sink of all packets (BS) with the help of traffic analysis if the analysis countermeasures are not applied to the WSN. Therefore, it is very crucial to increase the privacy of the location of the base station in case of WSN's.

The entropy and GSAT traffic analysis attack models sheds light on the entropy and GSAT traffic analysis attack models, which are popularly used to chart out counter measures and validates their role in upping the BS's anonymity [6]. This paper is an effort to summarize the effectiveness of the above mentioned models from an adversary's point of view. Such evaluation enables assessing whether existing countermeasures as powerful as they are assumed. Additionally, we analyze different routing schemes in order to gauge their strength and weakness in exposing the network to the aforementioned traffic analysis models. The analysis is supported by simulation results.

This paper is organized as follows: Section 2 summarizes

the related work. In Section 3, we analyze the commonly used traffic analysis attack models. Section 4 describes the case study. In Section 5, we evaluate the performance of the case study through simulation. Finally, Section 6 concludes the paper and gives directions for future research in this area.

II. RELATED WORK

Base-station anonymity techniques have been explored in multiple bodies of work [7]–[10]. Some solution employed more than one BS. For example, Taj et al [7] proposed a method for boosting anonymity by employing two BS in a hidden area, with a BS working as backup and the other BS is a regular functioning station. El-Badry and Younis [8] proposed a technique called MAG which exploits the presence of multiple BSs in the network to dynamically manage the traffic pattern. Game theory is utilized to determine the volume and destination of the traffic so that the variance in the location anonymity over all BSs is reduced. Ren and Younis [9], [10] explains how the anonymity of the BS nodes can be boosted for protecting them against threats in three different ways. They investigated the deployment of multiple BS nodes, the mobility of BS and forming clusters, and analyzed the impact of the BS multiplicity and mobility on anonymity. It was shown that exploiting the mobility of the BS and increase in the count of the base stations result in a major growth in the anonymity and also help in spreading of traffic and avoiding the formation of hot spots surrounding the Base Stations. However, employing multiple mobile base stations is not very helpful at all times as it might result in exposing all base-stations.

Instead of deploying multiple BS, some work tried to create fake sink instead. As a countermeasure, Deng et. al. [2] generate a set-up of decorrelation packets for masking the area of a base station against traffic analysis attacks. They proposed a strategy where an adversary is mislead about the actual area of the base station by creating many hot spots where there is a high communication activity. The adequacy of these countermeasures against traffic analysis attacks is demonstrated by using the total entropy of the system and the total energy consumed evaluation criteria. Similarly, in the approach of [11] the BS anonymity is improved by introducing fake sinks and designating deceptive relays to misdirect the data traffic to these fake nodes rather than to the BS. They utilized a heuristic for deciding the most appropriate fake sink count and placement for a network. Other work by Baroutis and Younis [12] investigated three traffic analysis models that an adversary could apply to find the BS and pointed out their advantages and shortcomings. They additionally proposed an attack model whose purpose is to boost the adversary's efforts in locating the BS to reduce the traffic analysis's complexity.

Several techniques relied on disguising the BS as a sensor or relocate it within the network. [13]–[15]. For example, Acharya et al [13], [14] proposed two techniques. The first is projecting the base station as yet another sensor node that sends out data just to confuse the adversary. Another method makes the base station to relocate to a more hidden position in the network. They also proposed a methodology for boosting the anonymity of the BS by making an observation that the BS node is simply one more sensor node sending information and therefore confound the adversary. The second method makes the base station to relocate to a more hidden position in the network. Three models – evidence theory model, GSAT test, entropy-based model have been used to evaluate the obscurity of the BS.

Some countermeasures try to carefully set the routing topology to boost the BS anonymity. For example, Alsemairi and Younis [16] form mesh based topology where the nodes are grouped into clusters, each has a designated cluster-head, CH. A mesh like structure is established among the CHs and including the BS, where each CH forwards the aggregated data from its cluster the inter-CH path. At that point, the BS forwards the aggregated data too with the goal that it shows up as one of the CHs. Other work by Ward et. al. [17]–[19] presented an approach to increase the BS anonymity through implementing distributed beam forming in a WSN. Evidence theory analysis has been used to examine the effect of the distributed beam forming technique on improving BS anonymity.

III. TRAFFIC ANALYSIS ATTACK MODELS

This section highlights popular traffic analysis attack models. The working of an adversary against the attack models to locate the base station and how they are also used as counter measures in various models are discussed.

A. Entropy and Traffic Volume

The Entropy model uses Shanon's information theory for measuring the randomness present within a network. [20]. Many researchers utilize this model to assess anonymity. [21], [22]. The entropy measure captures the traffic distribution in the network. Essentially, the sensor nodes are spread all through the deployment region of a WSN. An adversary can divide the whole deployment region into N cells and begin tracking transmissions from every cell independently. The adversary then assigns every cell a probability of having a BS. Let p_i be the probability at time t that a cell i contains the BS where $i = 0, 1, 2, \dots, N - 1$. An entropy value $H(x)$ can be calculated by the following equation given in [23]:

$$H(x) = - \sum_{i=0}^{N-1} p_i \times [\log_2(p_i)] \quad (1)$$

At the beginning, the probability of finding the BS is $1/N$ and thus, the maximum entropy H_{max} can be attained by substituting P_i with $1/N$ in (1).

$$H_{max}(x) = - \sum_{i=0}^{N-1} \frac{1}{N} \times \left[\log_2 \left(\frac{1}{N} \right) \right] \quad (2)$$

By combining (1) and (2) we define the ratio degree as:

$$\text{Ratio Degree} = \frac{H(x)}{H_{max}(x)} \quad (3)$$

After monitoring the network for a while, the total number of packets transmitted within the network over a time period and the quantity of packets that the i -th cell receives is computed by the adversary. The BS anonymity can be calculated using (1) and given in (4) and (5).

$$H(x) = - \sum_{i=0}^{N-1} \frac{p_i}{M} \times \left[\log_2 \left(\frac{p_i}{M} \right) \right] \quad (4)$$

$$\frac{H(x)}{H_{max}(x)} = - \sum_{i=0}^{N-1} \frac{p_i}{M} \times \frac{\left[\log_2 \left(\frac{p_i}{M} \right) \right]}{\log_2 N} \quad (5)$$

Where, P_i represents the number of packets transmitted from i -th cell and M is the total number of packets transmitted in the whole network.

Consider a case describing how we can deduce the entropy as the attack model by considering an adversary which attempts to compute the base station's location by identifying the cell with the largest traffic volume and predicts the base station's accurate location. The traffic volume (TV) of a cell i can be calculated as follow:

$$TV(i) = \text{no of transm} \times \text{transm range} \times \text{packet size} \quad (6)$$

A crucial advantage of the TV analysis its straightforwardness as its complexity is linear in the number of cells. However, it endures many weaknesses. Initially, the probability p_i of a cell differs after some time and relies upon the traffic volume of that cell. In cases like, the transmission range not being similar for all nodes and there is a difference in the packet sizes, these attack models can be easily manipulated. It might also happen so that the cell an adversary chooses has a smaller size which will result in the base station to end up picking a node belonging to a different cell. This will result in wrong assignment of the higher p_i cells close to the BS, and not the BS cell itself. In most of the cases, a large cell size results in a greater probability of identifying the base station cells with the help of this attack model.

B. GSAT Test

GSAT is a form of a testing tool which computes the average number of steps an adversary takes hopping between

cells before discovering the BS. [6]. The GSAT algorithm is utilized by the adversary to perform a local search in a greedy manner. The goal of the search is to identify the radio transmission hot spots and slowly progresses to the location where the base station is present. At first, the adversary begins from a random cell and monitors radio transmission activities inside its cell, which incorporates its own cell and all the neighboring cells, for a specific time frame. During this time, the adversary shifts to the adjacent cell with the maximum number of transmission activities to locate the BS. In case the adversary is unable to locate the BS in the cell with the highest transmission activities, this could correspond to a local maximum. Therefore, the adversary randomly chooses an adjacent cell to shift to. When the BS is reached, the greedy search is called off. The number of moves that the adversary takes until arriving at the BS represents the GSAT number. The more the network traffic is evenly distributed higher the GSAT number the adversary gets. At any time t , the GSAT score of a cell i is defined as:

$$G(i, t) = \frac{\text{No of cell visits}}{\text{No of total moves}} \quad (7)$$

The GSAT score of all cells at time t should sum up to 1 and given in (8):

$$\sum_i^n G(i, t) = 1, \text{ where } n \text{ is the total number of cells.} \quad (8)$$

The main advantage of the GSAT test is its implementation simplicity. However, it suffers quite a few shortcomings such as if by any chance the adversary has occupied a cell multiple times, then it is an indication of a high possibility of a base station to be located in the neighbourhood. Furthermore, the nodes that are away from the BS can inject redundant traffic and boost the anonymity of the BS. Additionally, it can delay the convergence of GSAT-based attacks significantly especially with numerous local maxima since it depends on not only the traffic distribution but on the cell size, number of cells, the starting cell and the number of local maxima.

IV. THE CASE STUDY

A WSN comprises various sensor nodes and a single BS, which are randomly distributed in an area. The sensor nodes monitor the environment in their zones by measuring the environmental conditions and send the measurement packet to the BS over multi-hop paths. An adversary can pursue hop-by-hop tracing to find the base station if there is a continual dissemination of packets from the source to the base station on a fixed path. Hence there is a need to achieve the anonymity of the BS is to randomize the delivery path between the sensor nodes and the BS. Therefore, in our case study, we select two routing schemes which are the Forward Random Walk scheme (FRW) and the Dynamic Bidirectional Tree (DBT)

scheme [24] in order to evaluate the traffic analysis attack models from an adversary's point of view.

A. The Forward Random Walk Scheme

As per the forward random walk scheme, it is required that every node has to get its hop count to the BS. This can be achieved by getting the Base-Station to send a hello message that gets flooded through the network. While being flooded, the number of hops will be noted. A node receiving multiple copies of the hello message can know the shortest path. In the FRW scheme, each node divides its neighbors into the nearer list, equivalent list, and further list. To send the packet, a node will randomly choose a neighbor from its forward list as the next-hop until reaching to the BS. Figure 1 depicts one of the delivery paths for the message under the FRW schemes, i.e, from the source sensor to the BS. Any listing will be discarded as a possibility to obtain the next hop if it will result in diverging the packet away from the BS, causing the latency to increase. Thus, the packet will be transmitted along a forward random walk from source to BS. The FRW increases the BS anonymity by randomizing the delivery path. However, there is an inevitable increase in the latency as the FRW pursues a delivery path that is longer the shortest one.

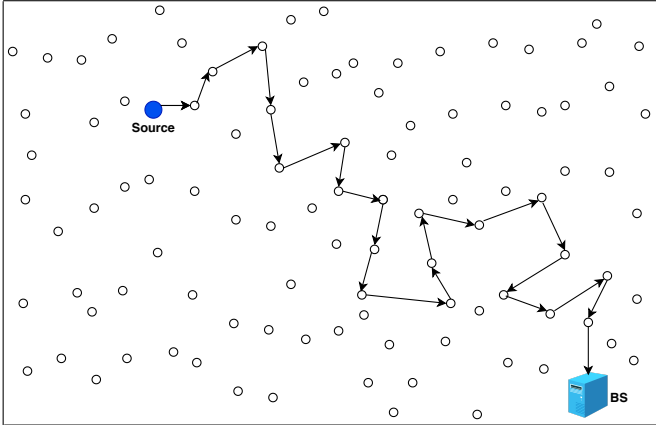


Figure 1: The scenario for the FRW scheme.

B. The Dynamic Bidirectional Tree (DBT) Scheme

Figure 2 shows one of the message delivery paths of the DBT scheme from the source to the BS where the black arrows represent transmissions of real messages and the red arrows represent the transmissions of dummy messages. The real messages are delivered along a forward random walk from source to the BS. Topological branches are designed along a forward random walk at the source side to increase the complexity for the adversary to trace the paths, and dummy messages are delivered from leaf nodes to the stalk nodes. As the adversary would follow the source by going in reverse the direction of the packet, the branches will diverge the adversary

from the genuine delivery path. Similarly, the topological branches along a forward random walk at the BS side are intended to secure the BS location protection. This is one way to deviate the adversary from the actual delivery path and to protect the base station location's privacy by sending dummy messages in the branches from the stalk nodes to the leaf nodes.

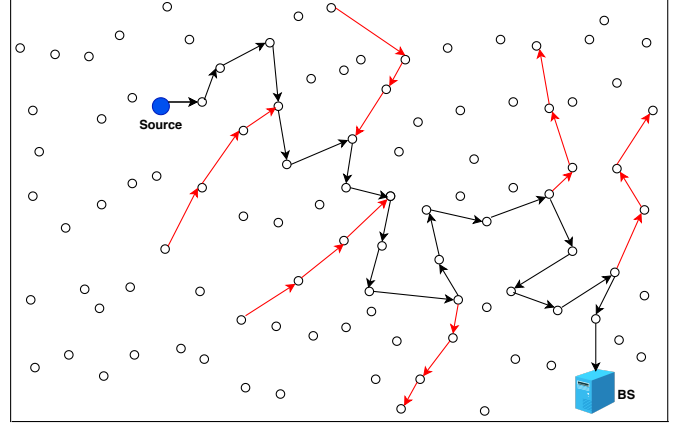


Figure 2: The scenario for the DBT scheme.

V. PERFORMANCE EVALUATION

In this section, we evaluate the FRW and DBT schemes in order to assess the entropy and GSAT traffic analysis attack models from an adversary's point of view. The performance of the FRW and DBT schemes was evaluated by using MATLAB. To test the performance of the FRW and DBT schemes under varying conditions, these schemes were evaluated assuming two different scenarios. In the first scenario, The GSAT values and entropy values have been calculated for FRW and DBT for a different number of nodes 200, 400, 600, 800, 1000 and for a different number of cells 4,8 and 16 cells under the setup of the size of the service region is fixed as 16x16 m2. In the second scenario, the service region has been changed to 2700* 9000 m2. The entropy, GSAT values have been calculated for 3000 nodes and 6000 nodes and for a different number of cells 4,8 and 16 cells. Furthermore, the energy consumption and the delay have been calculated for 3000 nodes.

In the two aforementioned scenarios, the results reflect the average over 1000 runs in order to achieve a 95% confidence interval and in each run, the source will be selected randomly and start sending the packet to the BS by using FRW and DBT schemes.

The end-to-end latency (L) and the energy consumption (EC) of the FRW scheme can be calculated as follow:

$$L, EC = \sum_{s=1}^{H_{BS}} HOP_{count}(s) \quad (9)$$

where L and EC of the FRW are equal to the hop counts from the source to the BS.

The end-to-end latency (L) of the DBT scheme can be computed by using equation (9) while the energy consumption (EC) of the DBT scheme can be calculated as follow:

$$EC = \sum_{s=1}^{H_{BS}} HOP_{count}(s) + 0.5 \times HOP_{count}(s) \times 3 \quad (10)$$

Where 3 is the number of the dummy packets that send by half of nodes from the source to the BS.

Figure 3 shows the results for the GSAT test for scenario 1. Figure 3(a) and Figure 3(b) display the GSAT value for the FRW scheme and the DBT scheme, respectively. As the number of nodes and cells increases, it can be observed that the GSAT value is reduced. For example, with 200 nodes and 4 cells, the GSAT is two thirds in Figure 3(a) and Figure 3(b), whereas with 1000 nodes and 16 cells it is about 0.3 in Figure 3(a), and zero in Figure 3(b). Therefore, the FRW and DBT schemes are effective in increasing the BS anonymity and the GSAT model is failed against these schemes, however, the DBT is more effective than the FRW in increasing the BS anonymity, especially with large cells number.

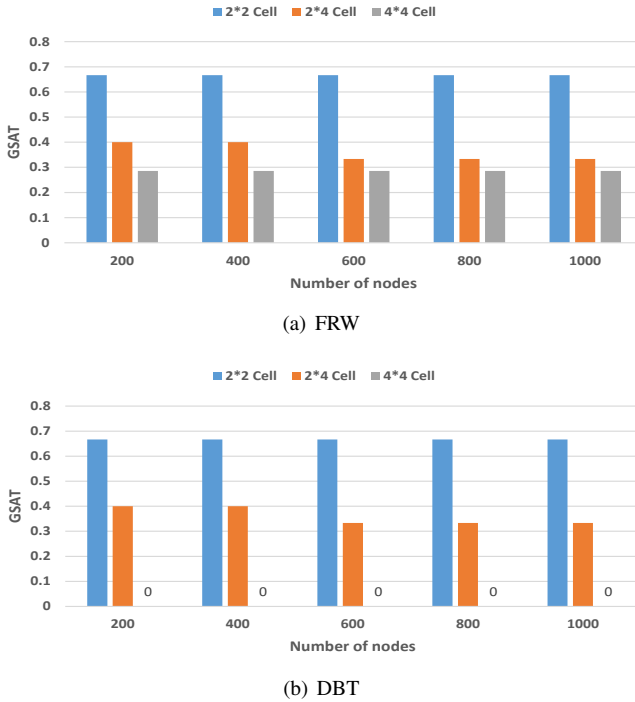


Figure 3: GSAT for (a) FRW and (b) DBT (for scenario 1).

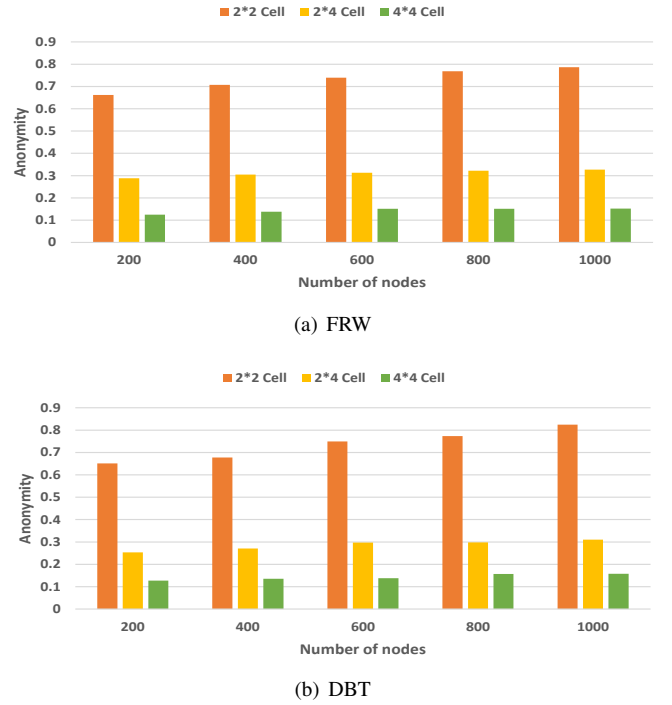


Figure 4: Entropy for (a) FRW and (b) DBT (for scenario 1).

Figure 4 displays the results for the entropy for scenario 1. Figure 4(a) and Figure 4(b) show the anonymity value for the FRW scheme and the DBT scheme, respectively. It can be observed that the anonymity value is increased as the number of nodes increases and the anonymity value is decreased as the number of cells increases. For instance in Figure 4(a) and Figure 4(b), with 200 nodes and 4 cells, the anonymity is two thirds, whereas with 1000 nodes and 16 cells it is about 0.15. Figure 4 demonstrates that the entropy model is failed against the FRW and DBT schemes and these schemes are able to increase the BS anonymity, particularly with large cells number.

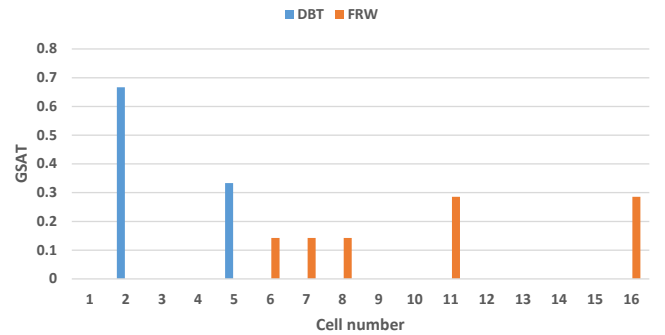


Figure 5: The GSAT value for each cell.

Figure 5 shows the GSAT value for each cell for the FRW and the DBT schemes for 1000 nodes and 16 cells. The blue bars present the GSAT value for each cell for the DBT scheme and the orange bars present the GSAT value for each cell for the FRW scheme. It can be observed that the GSAT value for the FRW is about 0.15 for cell 6, cell 7 and cell 8 and is about 0.28 for cell 11 and cell 16 and zeros for the other cells. This means the adversary will think that the BS is located either inside cell 11 or cell 16 while in fact it is located in cell 16. Whereas the GSAT value for the DTB is about two thirds for cell 2 and one third for cell 5 and zeros for the other cells. This means the adversary will think that the BS is located inside cell 2 while in fact it is located in cell 16. Figure 5 demonstrates that the GSAT model is failed against the FRW and DBT schemes and these schemes are able to increase the BS anonymity. However, the DBT is more effective than the FRW in increasing the BS anonymity, especially with large cells number.

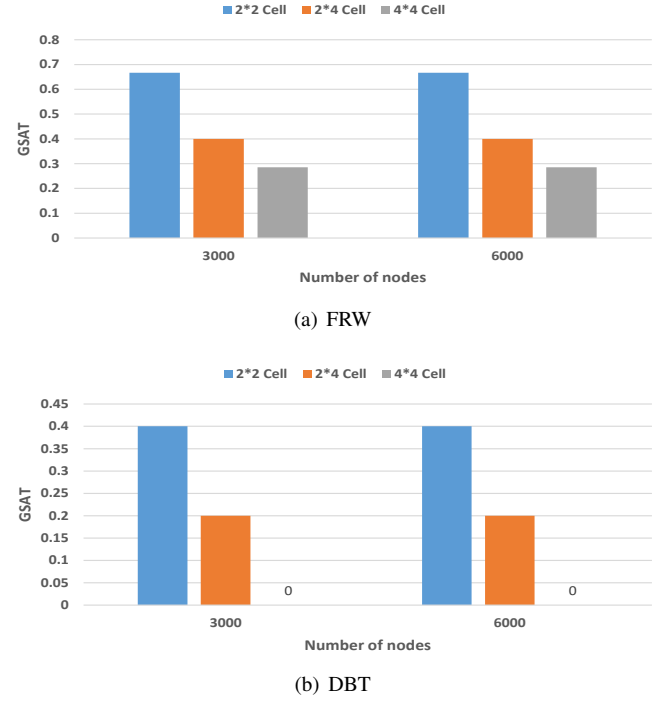


Figure 6: gsat for (a) FRW and (b) DBT (for scenario 2).

Figure 6 shows the results for the GSAT test for scenario 2. Figure 6(a) and Figure 6(b) display the GSAT value for the FRW scheme and the DBT scheme, respectively. It can be observed that the GSAT value is reduced as the number of nodes and cells increases. For example, with 3000 nodes and 4 cells, the GSAT is two thirds in Figure 6(a) and 0.4 in Figure 6(b), whereas with 6000 nodes and 16 cells it is about 0.3 in Figure 6(a), and zero in Figure 6(b). Therefore, the FRW and DBT schemes are effective in increasing the BS anonymity even with large deployment area with high density and the GSAT model is failed against these schemes, however, the DBT is more effective than the FRW in increasing the BS anonymity, especially with high-density network and large cells number.



Figure 7: Entropy for (a) FRW and (b) DBT (for scenario 2).

Figure 7 displays the results for the entropy for scenario 2. Figure 7(a) and Figure 7(b) show the anonymity value for the FRW scheme and the DBT scheme, respectively. It can be observed that the anonymity value is decreased as the number of nodes and cells increases. For instance in Figure 7(a) and Figure 7(b), with 300 nodes and 4 cells, the anonymity is 1, whereas with 6000 nodes and 16 cells it is about one third. Figure 7 demonstrates that the entropy model is failed against the FRW and DBT schemes and these schemes are able to increase the BS anonymity even with a large deployment area with high density.

Figure 8 shows the energy consumption for the Shortest Path (SP), the Forward Random Walk (FRW) and the Dynamic Bidirectional Tree (DBT) schemes. The SP scheme consumes the least amount of energy as it only delivers real messages along the shortest path and does not support creation of dummy messages. The FRW scheme consumes energy more than the SP scheme and less than the DBT scheme because of the explanation that it doesn't create any dummy message. The DBT scheme consumes the largest amount of energy as it possess more branches in comparison to the other schemes. Obviously, the DBT scheme is more efficient for boosting the BS anonymity than the FRW scheme and the SP scheme. However, it consumes energy more than the SP and FRW schemes.

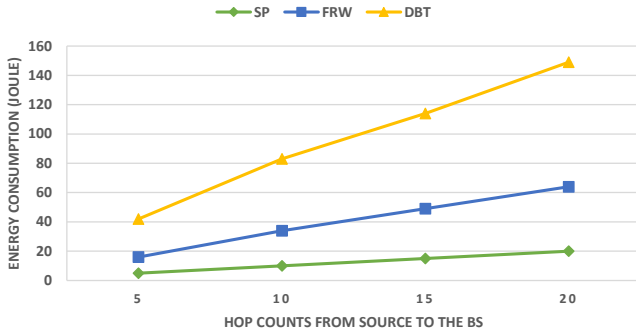


Figure 8: The Energy Consumption.

Figure 9 shows the end-to-end latency for the Shortest Path (SP), the Forward Random Walk (FRW) and the Dynamic Bidirectional Tree (DBT) schemes. The SP scheme achieves the shortest end-to-end latency since the real messages are delivered along the shortest path from source to the BS. The end-to-end latency in the FRW scheme and the DBT scheme is similar since the real messages in these two schemes are delivered along the forward random walk path. Clearly, the DBT scheme is more efficient for boosting the BS anonymity than the FRW scheme and the SP scheme. However, it achieves end-to-end latency similar to the FRW scheme but higher than the SP scheme.

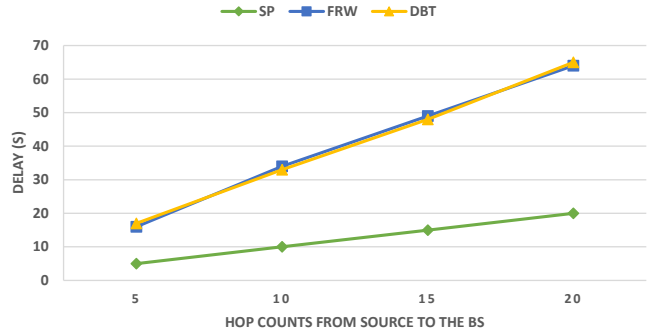


Figure 9: The End-to-End Latency .

VI. CONCLUSIONS

In this paper, we have analyzed the traffic analysis attack models (the entropy and GSAT test) and pointed out their strengths and weaknesses. Additionally, we have evaluated two routing schemes (the FRW and the DBT) in order to assess these models from an adversary's point of view. The simulation results showed that these models are failed against the FRW and DBT schemes and these schemes were able to increase the BS anonymity. The results demonstrated that the DBT scheme was more efficient for boosting the BS anonymity than the FRW but it consumes energy more than the FRW and achieves the same end-to-end latency that the FRW achieves. As future work, we plan to develop a mathematical model in order to find the optimal fake sink's placement for a network and solve that model by using a suitable solver. Furthermore, we plan to design new metrics can be used to gauge the effectiveness of anti-traffic analysis techniques. Finally, to confirm practicality, an empirical experiment needs to be carried out, in order to test the BS anonymity under various real-life conditions.

REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [2] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 159–186, 2006.
- [3] J. Kong, X. Hong, and M. Gerla, "An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 8, pp. 888–902, 2007.
- [4] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1501–1514, 2009.
- [5] P. Venkitasubramaniam, T. He, L. Tong, and S. B. Wicker, "Toward an analytical approach to anonymous wireless networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 140–146, 2008.
- [6] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE, 2005, pp. 113–126.

- [7] F. Taj, S. Anwar, M. Imran, and I. Ullah, "Anonymity of base station in wireless sensor network via backup base station," *International Journal of Computer Science and Information Security*, vol. 14, no. 6, p. 148, 2016.
- [8] R. El-Badry and M. F. Younis, "Providing location anonymity in a multi-base station wireless sensor network," in *ICC*, 2012, pp. 157–161.
- [9] Z. Ren and M. Younis, "Effect of mobility and count of base-stations on the anonymity of wireless sensor networks," in *2011 7th International Wireless Communications and Mobile Computing Conference*. IEEE, 2011, pp. 436–441.
- [10] Z. Ren and M. Younis, "Exploiting architectural techniques for boosting base-station anonymity in wireless sensor networks," *International Journal of Sensor Networks*, vol. 11, no. 4, pp. 215–227, 2012.
- [11] N. Baroutis and M. Younis, "Using fake sinks and deceptive relays to boost base-station anonymity in wireless sensor network," in *2015 IEEE 40th Conference on Local Computer Networks (LCN)*. IEEE, 2015, pp. 109–116.
- [12] N. Baroutis and M. Younis, "A novel traffic analysis attack model and base-station anonymity metrics for wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 18, pp. 5892–5907, 2016.
- [13] U. Acharya and M. Younis, "An approach for increasing base-station anonymity in sensor networks," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.
- [14] U. Acharya and M. Younis, "Increasing base-station anonymity in wireless sensor networks," *Ad Hoc Networks*, vol. 8, no. 8, pp. 791–809, 2010.
- [15] Y. A. Bangash, L.-F. Zeng, and D. Feng, "Mimibs: Mimicking base-station to provide location privacy protection in wireless sensor networks," *Journal of Computer Science and Technology*, vol. 32, no. 5, pp. 991–1007, 2017.
- [16] S. Alsemairi and M. Younis, "Cross-layer technique for boosting base-station anonymity in wireless sensor networks," *International Journal of Communication Systems*, vol. 30, no. 13, p. e3280, 2017.
- [17] J. R. Ward and M. Younis, "On the use of distributed beamforming to increase base station anonymity in wireless sensor networks," in *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2013, pp. 1–7.
- [18] J. R. Ward and M. Younis, "Increasing base station anonymity using distributed beamforming," *Ad Hoc Networks*, vol. 32, pp. 53–80, 2015.
- [19] J. R. Ward and M. Younis, "A metric for evaluating base station anonymity in acknowledgement-based wireless sensor networks," in *2014 IEEE Military Communications Conference*. IEEE, 2014, pp. 216–221.
- [20] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [21] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *International Workshop on Privacy Enhancing Technologies*. Springer, 2002, pp. 54–68.
- [22] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *International Workshop on Privacy Enhancing Technologies*. Springer, 2002, pp. 41–53.
- [23] T.-J. Chan, C.-M. Chen, Y.-F. Huang, J.-Y. Lin, and T.-R. Chen, "Optimal cluster number selection in ad-hoc wireless sensor networks," *WSEAS transactions on Communications*, vol. 7, no. 8, pp. 837–846, 2008.
- [24] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.