私立東海大學資訊工程學系研究所

碩士論文

指導教授：林祝興 博士

共同指導教授：劉榮春 博士

無線感測網路基地台匿蹤及網路壽命延長之研究

On Sink Anonymity and Lifetime Improvement in Wireless Sensor Networks

研究生：曹逸竹

(Yi-Chu Tsao)

中　華　民　國　一　百　年　六　月

Abstract

In wireless sensor networks (WSN), the base station plays an important role which needs to collect data from all sensor nodes deployed in a wide region. Once the base station is destroyed, it cannot work normally, i.e., it cannot receive data from sensor nodes, and also cannot send data to the terminal server. The wireless sensor networks will lose its function of collecting data. Any malicious person can locate the base station, then attack or destroy it to damage the entire wireless sensor network. How to protect location of the base station and make it hard for the malicious person to find the base station is the primary objective of this study. Meanwhile, when the range of wireless sensor network becomes larger, the routing path becomes longer and packets need to go through many nodes to reach the base station, and the node energy will be consumed very fast. In order to take into account the base station and the lifetime of the network, we employ a mobile base station scheme to enhance the anonymity of base station and prolong the lifetime of wireless sensor networks by distributing traffic in networks.

In the simulations, we divided the wireless sensor networks into 3x3, and 5x5 cells. Experimental results show that our proposed method not only increases the anonymity of the base station but also greatly prolongs the lifetime of the network. We also observe that when the scale of the nodes of the network becomes larger, the method is more effective. We can also adjust the frequency of movement as 30 minutes, 60 minutes, or 90 minute to improve the anonymity of base station as needed.

Keywords: WSN, mobile sink, privacy protection, anonymity, lifetime

摘要

在無線感測網路中，基地台 (Base station) 扮演重要的角色，基地台負責收集無線感測網路中所有感測節點 (Sensor nodes) 的資料，由此可知，一旦基地台遭受到破壞便無法正常運作以接收感測節點的資料，同時也無法傳送資料至後端主機進行處理，此無線感測網路將會失去作用，因此基地台成為惡意人士的首要攻擊目標。惡意人士欲攻擊基地台，必須先找出基地台的位置，才能對基地台加以攻擊或破壞，以達到摧毀無線感測網路的目的。如何保護基地台的位置不被洩漏，且使敵人不容易找出基地台的位置，是本研究的首要目標。另一方面，無線感測網路的規模越大，則資料的傳送路徑將越長，封包必須經過更多節點才能送達基地台，因此節點的電力將迅速地消耗。為了兼顧基地台的匿蹤性以及網路的使用壽命，我們提出可增進基地台匿蹤性及延長網路壽命的方法─移動式基地台，來達到本研究目的。

本研究的模擬實驗將網路劃分為 3x3 及 5x5 區塊的網路，實驗結果顯示，透過移動式基地台，不但能成功提升基地台的匿蹤性，使敵人不易迅速地找到基地台，且大幅提升網路的使用壽命至少一倍以上，若網路規模越大則提升的效果越明顯。此研究方法還可依照需求，來選擇不同的基地台移動時間間隔，讓基地台更為安全且同時延長網路壽命，成功達到雙贏的目的。

關鍵詞：無線感測網路，移動式基地台，隱私保護，匿蹤性，網路壽命

致謝

在研究所學習的歲月中，有苦有悲亦有喜有樂。由於大學所學與研究所的專業在不同領域，因此對於我而言，是一個全新的開始！自碩一進入實驗室後，以 ZigBee 系統做室內定位是我第一個全心投入且收穫最多的研究，這開啟了我對資工領域更深入的認識，也間接確立我的研究主題。

這篇論文能順利地完成，要感謝的師長以及朋友實在太多了！首先要感謝我的指導老師林祝興教授的諄諄教誨，老師不但重視學生在專業領域的學識，也給了我們非常大的發揮空間，讓我們能自由地徜徉在學術領域中，同時也要感謝劉榮春教授，有了劉老師的大力幫忙與指導，使本篇論文的內容更加完美與充實。再來是陪伴我最久的同學─哲維、冠翰，與他們相處總是感覺輕鬆自在，彼此相互砥礪成長；年輕有活力的學弟妹們─信斌、棠濰、泓彥與詩蓓，帶給了實驗室許多歡樂氣息，讓我每天離開實驗室都有種依依不捨的感覺；此外更要感謝在職班的學長們─昇興，建興，書源，子見與桂綸，因受他們的鼓勵和對做學問積極拼搏的態度，我的論文才得以順利完成。還有那總是比我還加倍努力的室友兼房東─介妤，身為在職碩士生，她必須兼顧學業與事業，看見她認真進取的學習態度，使我不致懈怠。最後，感謝母親一直以來對我的包容與支持，在完成論文進入人生另一個里程碑之際，我必將持續努力學習，以慰父親生前殷殷期許。

Contents List

Figure List

Table List

Chapter 1 Introduction

In recent years as the rapid development of wireless networks, and advanced micro-electromechanical manufacturing technology, which not only significantly reduce the cost of wireless devices, but also miniaturize the device, the wireless device is suitable for environmental detection and monitoring, and as the result, the applications of wireless technology are more extensive. The wireless network standards─IEEE802.15.4 commonly known as wireless sensor network (WSN) [1], because it can be used in many areas such as the office building, hospital, home environment, wildlife habitat or military establishment. With its technology to realize indoor positioning, data sensing (for light, sound, vibration and temperature, etc.) and collection, the applications of WSN is unlimited.

In wireless sensor network, the base station is the most important device that is responsible for collecting sensor data from all nodes. It can be seen that once the base station does not operate properly, the sensor nodes will not be able to forward messages to the base station, the base station will be also unable to send data to the server, and the network will lose the function of collecting data. For this reason, the base station is vulnerable to malicious actions that either remotely attacks the base station through networks, or finds actual position of the base station and damages it directly. Above mentioned malicious actions do not require take down all the sensors in wireless sensor networks, and so these methods of attack are very economical and save time and cost. Therefore, to prevent leakage of the location of the base station is the primary objective of high-security wireless sensor networks, which ensure that base stations are less vulnerable to

attacks and provide normal functions and services.

1.1 The anonymity of base station

From the point of view of the attackers, how to find the location of the base station in wireless sensor network is the primary objective that must be addressed. Such attackers may have powerful equipments, such as a high-power antenna, or a laptop which has enormous computing capability. They maybe go around the environment for eavesdropping packets in WSN, and analyze the network traffic to find the location of the base station, as shown in Figure 1.

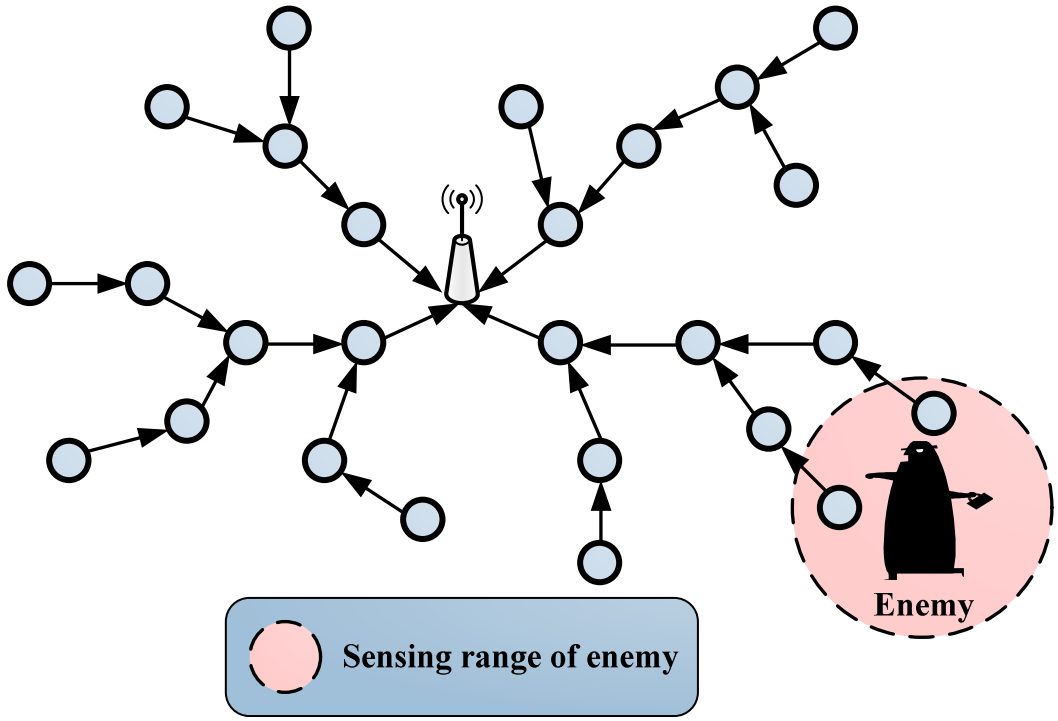


Figure 1: Description of activities of the malicious person

Wireless sensor networks have two characteristics: the base station in wireless sensor networks must collect information from other sensor nodes; and

each sensor node needs to send data by a fixed multi-hop path to transmit packets of data to the base station. Based on these two characteristics, a malicious person can observe the data packets flow in the network to estimate the location of the base station. As shown in Fig. 2, the neighbors of the base station are responsible to forward packets to the other sensor nodes. In other words, all routing paths are joined at the area around the base station. Therefore, nodes around the base station receive and transmit more packets than others, and these nodes are responsible to the majority of network traffic and so they show frequent activities. For this reason, the area around the base station tends to attract the attention of malicious persons. Even if the range of WSN are deployed very widely, as long as the attackers can keep track of flows of the particular packet, and analyze the activity of nodes step by step, they will be able to locate the base station.

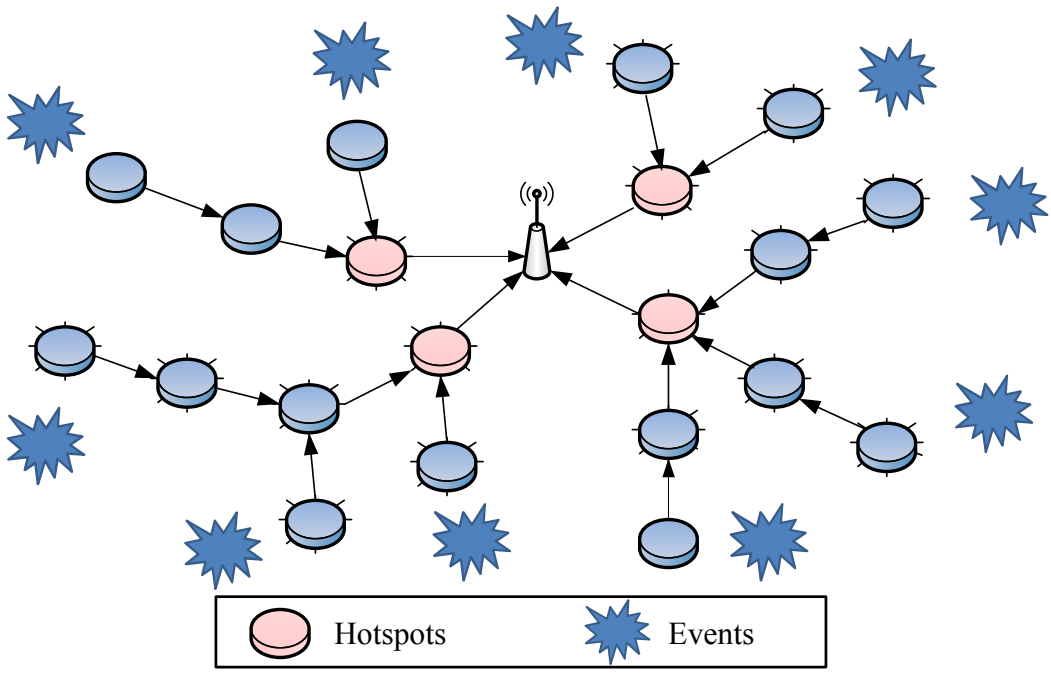


Figure 2: Data transfer in WSN

In order to avoid exposing the location of sink, many researchers propose to overcome this problem by increasing the anonymity of sink [2-7]. A clear definition of anonymity, including identity, role, and position of the base station is also given [8]. Several mathematical models used to estimate anonymity can be applied directly to existing WSN. In addition, to enhance the anonymity of the base station [9-11], many methods are proposed, for example, k-anonymity, and Base-station Anonymity (BAR) boost the base station anonymity via re-transmission [9][10]. Acharya et al. employed packet retransmission to randomly or periodically send packets from the base station to distribute traffic flow and make it hard to decide whether a region is near the base station or not [4]. However, such practice of packets retransmission causes the neighbors of the base station subject to more traffic. It not only increases additional communication costs, but also leads to consumption of limited energy of the neighboring nodes of the base station.

1.2 Prolonging lifetime in WSN by mobile sink

There are many ways to extend the life time of wireless sensor networks, through appropriate configuration of coverage of sensor nodes, or limitation of the antenna power to save power consumption. In recent years, many researchers have proposed the mobile base station method to extend the network lifetime and increase service time of WSN [12-19]. These researches assume that the base station is deployed in a mobility device, such as a vehicle, moving with a certain speed. So the base station can be periodically re-deployed to varied position. It

can move to areas with lower activity in order to distribute traffic flows in WSN, as shown in Figure 3, in which the base station makes a decision to move to a new location. Thus the original routing paths will change with the location of the base station, and WSN needs to re-generate new routing paths.

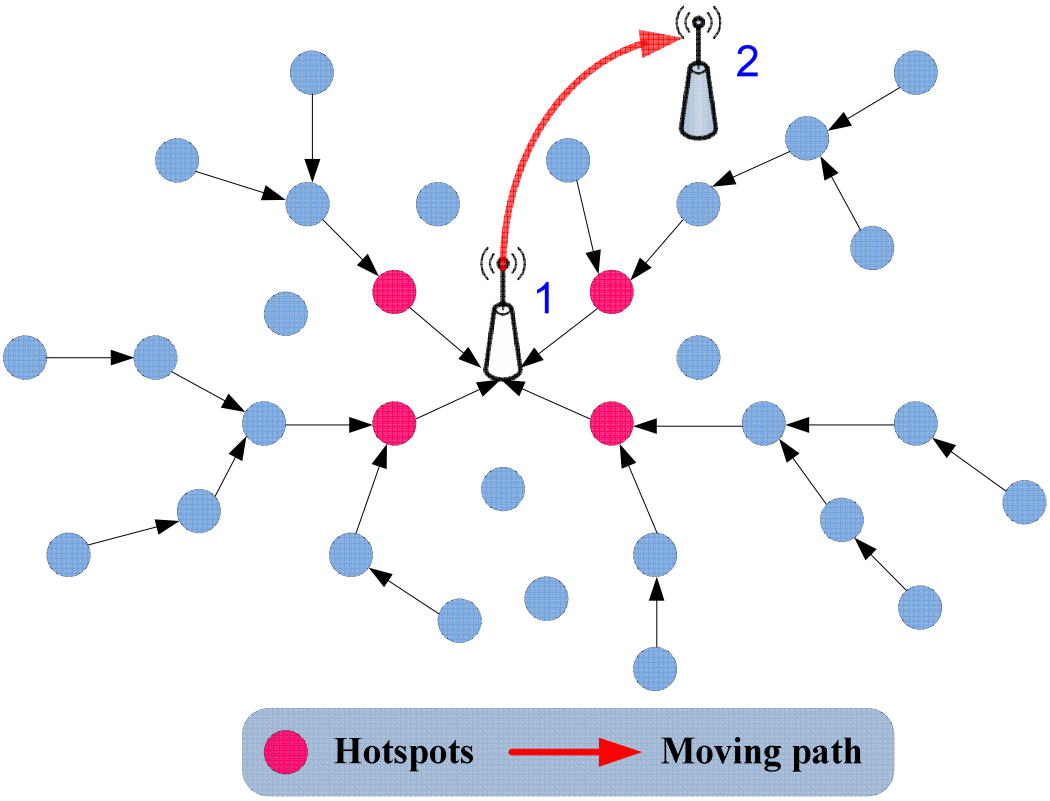


Figure 3: Description of mobile sink

There are two motives for re-locating the base station. First, it improves tracking difficulty by moving the base station. Second, it adjusts the distribution of network traffic to prolong the service time of WSN. To select the appropriate new location of the base station is a challenging problem, as stated in the following:

1. How: first of all, the system must decide how to control data traffic flow of

the entire wireless sensor network.

2. When: the base station need to decide when to re-locate to the new location.

3. Where: the base station should select its new location.

4. During the movement of the base station, how the sensor nodes forward data to the mobile base station is a complex problem due to the change of routing paths.

The mobile base station decides the suitable next location to adjust the status of wireless sensor networks by enhancing the anonymity of sink, or varying the routing paths of sensor nodes to extend the service lifetime of WSN.

In the process of moving the base station, the sensor nodes can not immediately get information of the new location of the base station, and the data routing path is not changed that will cause data packets loss since the data packets transmitted from nodes are not forwarded correctly to the base station. At the same time, the nodes also consume more energy for packet retransmissions. We propose a method to overcome this problem: sensor nodes stop transmitting data and wait for a while until the mobile base station reaches the new location. After configuring the base station with a new topology to receive data from sensor nodes, sensor nodes can re-forward data packets by the new routing path. This method reduces packet loss by delaying the time of forwarding packets to the base station and it extends the service lifetime of the target nodes.

1.3 The outline of this study

The rest parts of this thesis are arranged as follows. In the first section of Chapter 2, the background of the research will be discussed; in the second section of Chapter 2, strategies for movement of mobile base stations and strategies on improvement of the networks lifetime will be discussed. Chapter 3 illustrates the research method, including problem definition, and the strategy of the base station movement to achieve two advantages: high-anonymity WSN, and increase of the lifetime of the network. Chapter 4 shows the experimental environment setting and experimental results to prove that our proposed method can improve the anonymity of the base station and prolong and the network lifetime. Chapter 5 concludes this thesis by summarizing our study and discussing of the future work.

Chapter 2 Background

2.1 The wireless sensor network

A wireless sensor network consists of a lot of sensor nodes to monitor and measure sound, light, air vibration or temperature, etc. They also send data to the base station with simple computing and wireless communication capabilities. In order to achieve a large scale of deployment, the sensor nodes have low cost, low power, small size and easy to deploy features and they can be used in a hospital, in the military, the warehouse, and at home for management and automation. Nowadays, ZigBee is refered to the wireless sensor network, rather than Wireless Ad-hoc Network (WANET), although both have similar structure, but there are many different natures between them. The focus of this study is on the ZigBee applications.

Figure 4: Applications of ZigBee

In December 2004, the official version for the ZigBee 1.0 specification was released by the ZigBee Alliance [1]. The alliance was initially set up by Honeywell, Invensys, Mitsubishi, Motorola and Philips, and the number of alliance members so far has more than 200 companies and extends to 26 countries. The name idea of ZigBee is by the bees: the bee doing the Z-shaped fly to inform peers of the pollen. The development objective is to create the wireless network with a low data transfer rate, low power and low complexity. It can work for at least a few months or even for a year with a battery. The ZigBee has three characteristics, as detailed below:

1. Low power consumption

   The low data transfer rate of Zigbee devices let them send and receive data by less time. They are in the non-operating mode when the device is in the sleep mode. To send and receive data, they will wake up again. In the sleep mode, the device consumes very low power, and it allows ZigBee to operate on only batteries for several months or even up to one year.

2. High reliability

   ZigBee employs a collision avoidance mechanism on the MAC layer. When a node receives a packet, it sends a confirmation message to inform the sender. If the sender does not receive a confirmation message, which means that the packet collided with other packets, then it will retransmit the same packet. The collision avoidance mechanism increases

reliability of the transmission system.

3. High scalability

In order to achieve the aim of wide deployment, a ZigBee network can support up to 255 devices to each communication links; and the network can be expanded up to thousands or even tens of thousands of devices by using a ZigBee network coordinator.

ZigBee is a specification based on the IEEE 802.15.4 wireless standard that employs the standard of low-rate wireless personal area networks (LR-WPANs) such as physical layer (PHY) and media access control layer (MAC). ZigBee operates in three radio bands. The MAC layer provides flow control, network organization, and data encryption (AES-128) services. The radio band of its license-free radio channels and the application areas are as shown in Table 1, and its transmission range is from 10 to 75 meters.

Table 1: Operation bands of IEEE 802.15.4 specification

Operation Bands	**868.0-868.6 MHz**	**902-928 MHz**	**2.4-2.4835 GHz**
Area	Europe	Americas	Worldwide
Channels	1	10	16
Data rate	20 Kbps	40 Kbps	250 Kbps

While ZigBee and IEEE 802.15.4 architecture is similar, but there are some different as shown in figure 5. In November 2007, the Alliance completes development of ZigBee 2.0 specification to provide more function of networks.

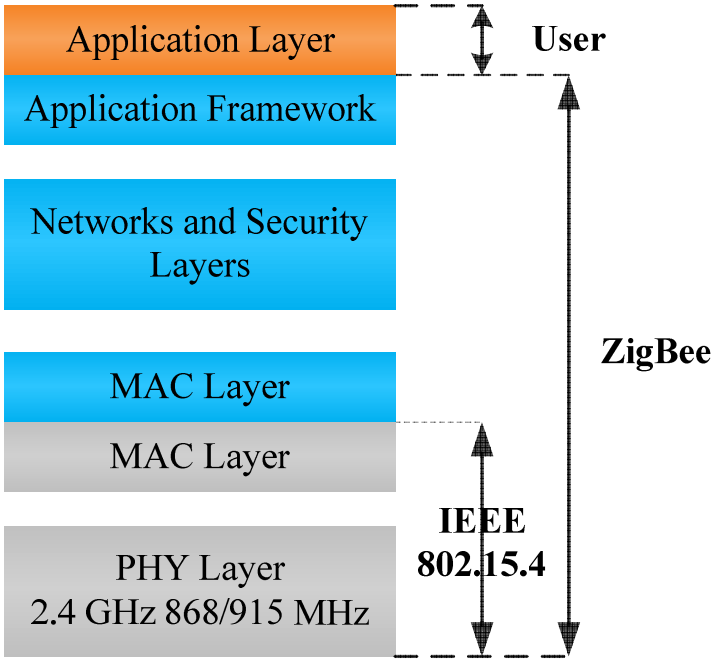


Figure 5: The relationship between IEEE 802.15.4 and ZigBee

ZigBee supports the star topology, mesh topology (also known as point to point), and cluster tree topology networks as shown in Figure 6. There are three types of network devices:

- ZigBee coordinator (ZC)

  It is the most power among these three devices. It can be used as the root of the network tree and can also be used as routers of the network. The coordinator has more memory than the other two types, and it has greatest computing and power supply abilities. There is only one coordinator in a network.

- ZigBee Router (ZR)

  The ZigBee router can act as a relay router as coordinator, but it has limited computing capacity and power. It can immediately communicate to all types of device, and relays data from other devices to the base station.

- ZigBee End Devices (ZED)

  It contains the least functions. A router can only communicate with parent nodes (ZigBee routers only), and it has least memory. So it is less expensive than the ZigBee coordinator and router. The end device cannot relay data from other devices to reduce the cost and setup complexity. It is suitable for simple applications because it can switch to the sleep mode to save energy.

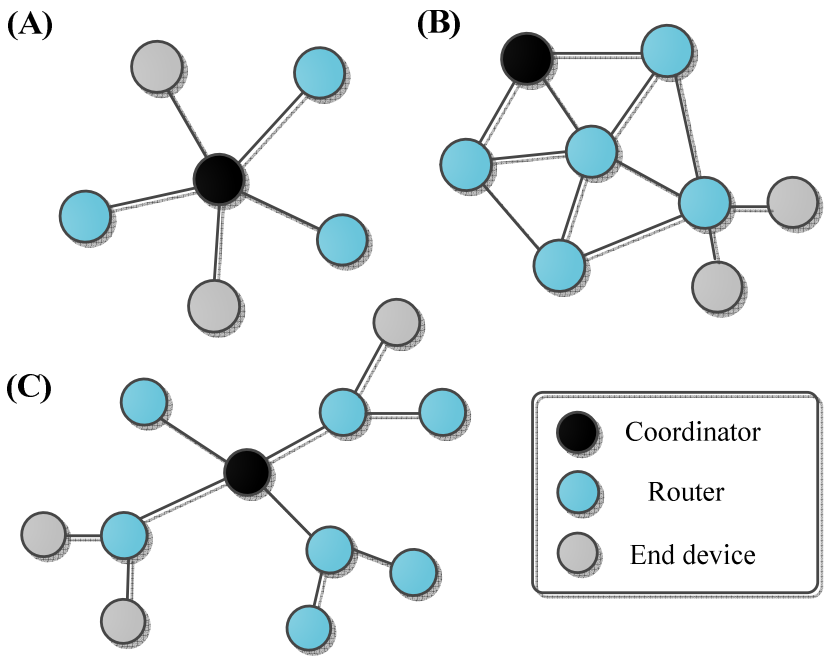


Figure 6: Topologies of ZigBee: (a) Star topology (b) Mesh topology (c) Cluster tree topology

In Figure 6 (a), the devices in a star topology directly communicate with the central coordinator of the network. In this case, the ZigBee coordinator is the most

powerful device in the network, and the other devices are only equipped with batteries to maintain operation. The star topology is more suitable for applications in smaller areas such as home. Figure 6 (b) shows that the mesh topology allows nodes transmit and relay by multi-hops to reach the ZigBee coordinator. The mesh topology provides high reliability structure with a scalable range. Figure 6 (c) shows a cluster tree topology, in which most devices are ZigBee routers. The ZigBee routers have communication links to ZigBee end devices as leaf nodes, and relay data to the ZigBee coordinator. The routers are responsible for communicating with the coordinator. There is only one coordinator for each network (the black node in Figure 6). The advantage of the cluster structure is that it can increase the range of the radio signal coverage for data communication.

2.2 Related works of privacy protection for base station

In the past wireless sensor network researches were focused on solving the energy consumption and reducing the computation problems, but in recent years, the privacy of the information transmission has gradually received attention. For wireless sensor networks to carry data through wireless radio signal, how to achieve privacy protection is a very challenging problem. This section describes related research and classifications of the privacy protection for the base station.

2.2.1 Classification of privacy protection in WSN

This section describes the classification of privacy protection technology. Li et al. divide the privacy protection into several categories [2], as shown in Figure

7. It shows two main categories: one for data privacy, the other for the context of privacy. The data privacy-oriented protection provides the security of data. On the other hand, the privacy is for the contextual information such as the location and time of packets sent, network traffic flow. Because the information of WSN is transmitted via the radio signal that may be eavesdropped by anyone, these two categories are likely to be attacked through the network analysis to obtain more information. Figure 8 describes the two attacks, namely data analysis attack and traffic analysis attack [2]. For the data analysis attack a compromised node is placed in the wireless sensor network to get the sensitive data by decrypting received packets. On the other hand, the data traffic analysis attack is not able to decrypt packets, in other words such attack can only track the traffic flow to analyze network characteristics by eavesdropping.

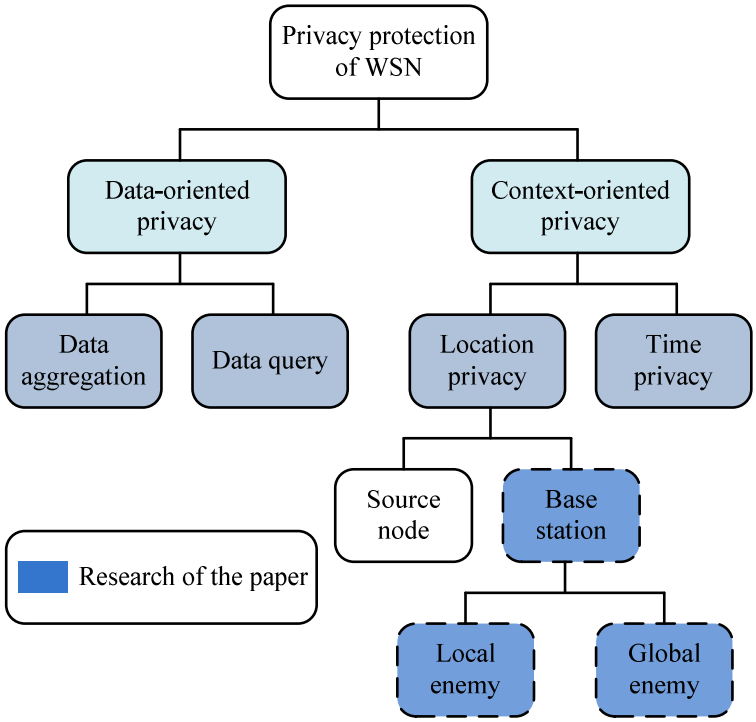


Figure 7: Privacy protection classification

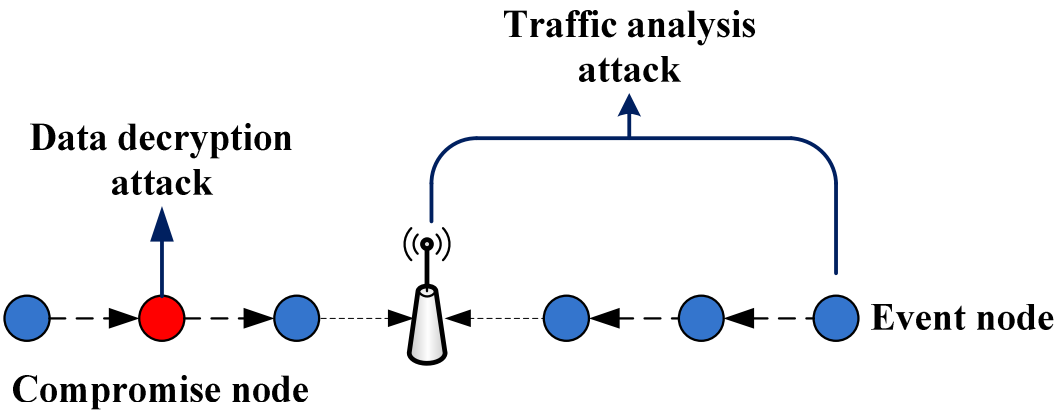


Figure 8: Two types of attacks on privacy protection

- The purpose of data-oriented privacy protection

The data-oriented privacy protection aims to protect the privacy of data content, the meaning of "data" is not just the information collected by nodes, but also includes other information such as query, and acknowledgement of received packet. As WSN is applied to monitor patient conditions, the sensed data of patient's blood pressure, heartbeat, body temperature, and the query message is produced by sensor nodes if the patient makes an urgent call. If such data and messages are eavesdropped by malicious persons who are interested in the patient, the patient’s safety may be in jeopardy.

Malicious people may come from different places and are generally divided into two types. The first type is the outside enemy, who eavesdrops the radio signal to get the packet, and so this type of enemy can be effectively prevented by employing traditional cryptographic schemes. The internal enemy is the second type of enemy who has powerful ability to crack sensor nodes, and put a compromised node to decrypt the received packets, So the

traditional cryptography cannot be used to effectively prevent such enemy.

- The purpose of context-oriented privacy protection

The context-oriented privacy protection allows protecting the characteristics of wireless sensor networks from readily exploiting by malicious person who is interested in the network. The characteristics include location information, events occurring time, or data transmitting time. In the wireless sensor network, there are important devices such as the base station, the cluster head and event nodes that need privacy protection to avoid leaking information of nodes locations to the enemy. Time of privacy ensures that the time of occurring events on sensor nodes is not leaked. If malicious person gets the event generation time of nodes, he may track or identify the event target, and even predict target movement without the need to understand the content of the packet.

Same as data-oriented privacy, the context-oriented privacy is subjected to the external and internal enemies. The existing researches have focused on how to guard against the external enemies. According to their capacity, the external enemies are classified as local and global enemies, as shown in Figure 9. With limited capacity for eavesdropping, the local enemies can just observe a small area of networks. In contrast, the global enemy is rather powerful, may be equipped with signal amplifiers, and thus has broader area for eavesdropping, even over the entire network.

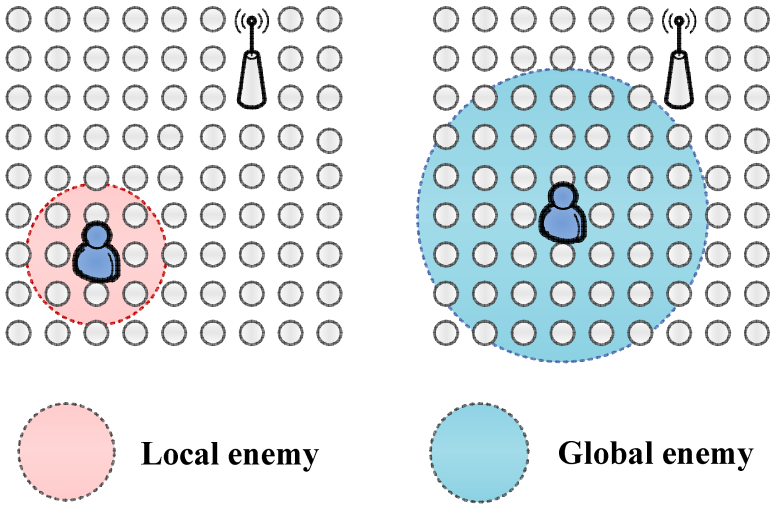


Figure 9: Distinct ability of two types of enemies

2.2.2 Privacy protection of base station

The base station not only is responsible for collecting the data from the sensors, but also is a gateway to the external network. In general, security schemes assume that the base station is safe, but once the base station is attacked by malicious person, it may fail to work and will impact the whole network. Hence, to keep the network work properly, base station security is very important. This section will introduce location privacy-related research of the base station to understand what technology can defend the local and global enemies.

2.2.2.1 Guard against local enemies

To protect the information of location of the base station to resist the local enemy, one needs to address two problems [5, 9, 10]:

- First, the data packets contain information of location of the base station,

the packets need to be encrypted by pair-wise key to hide information of the base station.

- Secondly, by eavesdropping the time of packet transmission, the local enemy can observe the relation between the sender and receiving nodes to infer the routing path and locate the base station by a complete routing path.

The first types of problems can be effectively overcome by use of cryptographic techniques. In contrast, to solve the second types of problems, researchers have proposed the following techniques.

1. Making changes in packet encoding by re-encryption

   The approach is similar to the anonymous routing of the wired networks. In 2006 Deng et al. proposed that packets can be re-encrypted during each transmission as shown in Figure 10 [5]. This mechanism avoids leakage of base station location by changing encoding of the same packet hop-by-hop, hence the enemy cannot trace the same packet through the routing path by eavesdropping.

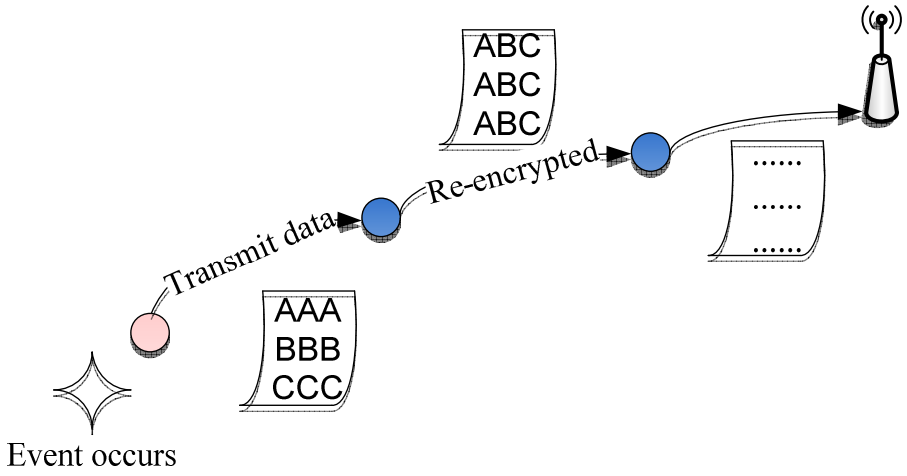


Figure 10: Re-encryption of the same content packet

2. Multi-neighbors routing scheme

Deng, R. Han, and S. Mishra et.al proposed a multi-neighbors routing scheme to distribute traffic load [5, 9, 10], as shown in Figure 11(b). That means the routing path of a packet has more than one paths, and every sensor can select one of its neighbors to relay a packet toward the base station. The scheme enhances security of information of location of the base station to prevent enemies from finding it through tracing a packet.

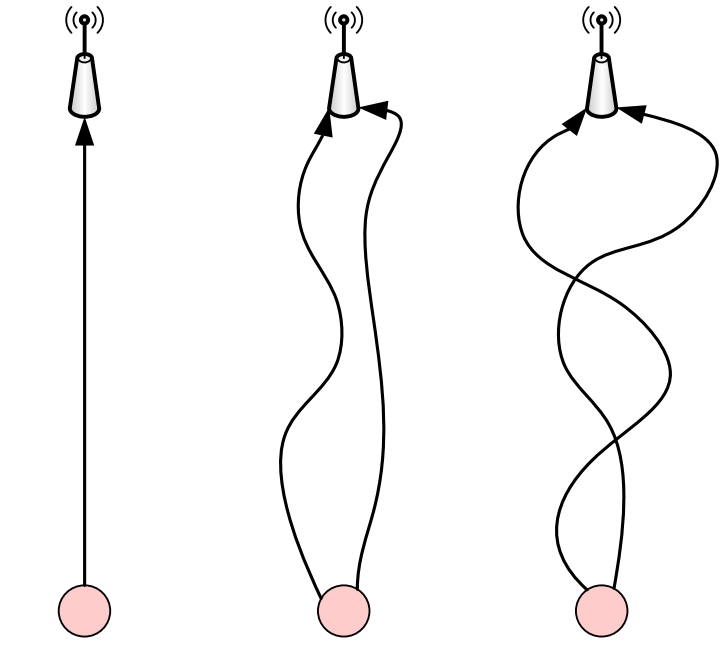


Figure 11: Technologies to resist traffic attack

3. Employment of random walk routing

Y. Jian et al. proposed a random walk routing that classifies neighbors into two types: the closer and farther neighbor respectively [11], as

shown in Figure 11(c). When the sensor node transmits data, it will pick one type of neighbor as the receiver. In addition, Deng et al. improved the random walk according to probability of picking neighbors [9], as shown in Figure 12. The scheme increases the difficulty of traffic analysis but may delay the time of data reaching the base station since the routing path may not be the shortest path.

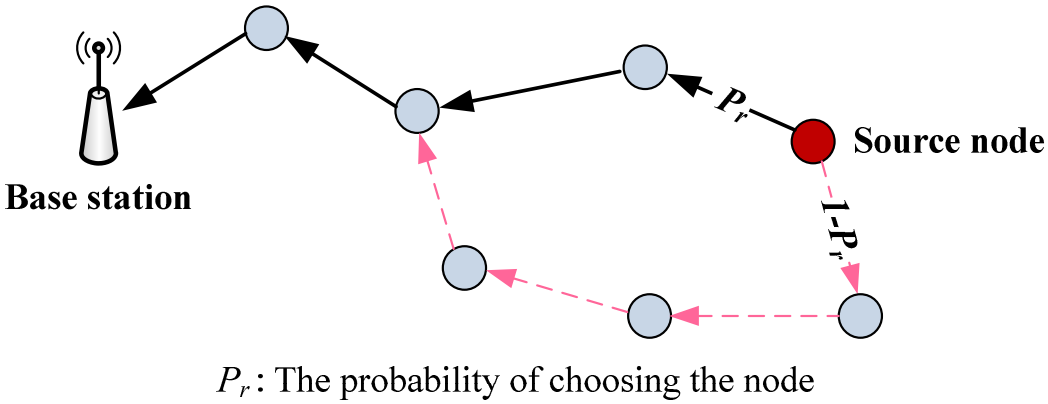


Figure 12: The random walk scheme with probability P_r

2.2.2.2 Guard from global enemies

The technologies mentioned above cannot effectively resist the powerful enemy who has capability of eavesdropping over broad area. The powerful enemy can even estimates the data transfer rate for each node, so he can detect the location of the base station easily. In order to resist the global enemies, dummy data and fabrication of fake base station locations are essential to confuse the judgments of the enemy. We discuss the relevant technologies as follows:

1. Covering up of traffic pattern by controlling data transmission rate:

High traffic flows of specific areas in wireless sensor network make the enemies easy to find location of the base station, since nodes near the base station not only transmit their own data but also relay data from other nodes to the base station. Therefore, researchers proposed to control the data transmission rate and the routing path to have a uniform data transmission rate on any area in the wireless sensor network.

2. Transmitting fake data:

   Since the enemies cannot distinguish actual data from fake data, nodes can generates fake data to disturb enemies to analyze real traffic pattern distributions. In this approach, when a sensor node transmits a data to the base station, its neighbors may send a fake data to further nodes. Figure 13 gives a clear illustration of this idea. Deng sets a probability P_c to send the fake data, and provides two sending approaches named as fractal propagation methods [9].

   - The first approach is to control P_c by the data transmission rate of a sensor node. If the transmission rate is high enough the probability P_c will be set for a lower value, and vice versa. The purpose is to average the traffic flow of each node.

   - Another approach is to imitate high volume data transmission areas, so there are many areas with high traffic volume. It lets enemies misjudge the location of the base station. But there is a drawback

of this approach, since extra power is consumed to produce camouflage information.

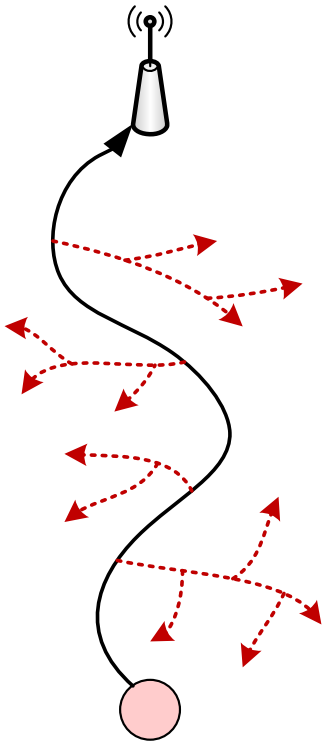


Figure 13: Transmitting fake data to disturb enemies

2.3 The research on mobile base station

2.3.1 The research on mobile base station

In general WSN applications, there is only one base station, and all the data packets from all the sensor nodes will converge to the base station. In this case, work load of nodes near the base station is greater than the farther nodes. The nodes consume energy fast in transmitting and receiving packets and become hotspots [20]. It causes networks to lose function. Although there are many

researches carried out to reduce energy consumption of nodes, but they still cannot properly manage the energy consumption of the overall network. Many researchers have proposed approaches to solve the hotspot problems as follows:

1. Many researchers proposed a routing protocol based on energy management [12]. The idea is that the node in hotspot will transfer some of the work load to minor nodes.

2. In general wireless sensor network applications, there is only one base station, but there are researchers believe that we can place more than one base station [12]. These base stations can cooperate with each other to distribute work load to improve the overall network lifetime.

3. In addition, the recent research trend for the wireless sensor network is toward mobile nodes. The mobile nodes transmit data to the base station in more convenient ways. Shah et al. proposed that the mobile node of sensing area can be a relay agent [21]. When incidents occur in the sensing area, sensor nodes transmit data to the mobile node, and then the mobile node will directly move to the area of the base station and relay data to the base station with a single hop to replace the multi-hop transmission path. This approach can save the energy of nodes.

   Kim et al. proposed a protocol—SEAD (Scalable Energy-Efficient Asynchronous Dissemination) based on Shah et al. [22]. They take advantage of tree-based topology and mobile base stations to resolve the

hotspot problem, redirect data flows, and balance the energy consumption of each node. Their experimental results show that deployment of mobile base stations is more energy efficient than the static base station. Many other researchers have shown that mobile base stations can solve the hotspot problems and balance energy consumption [12-20].

2.3.2 Research of mobile base station to prolong network lifetime

In this section, we take Z. Maria Wang's study for an example to explain the movement of location of the base station and the effect of retention time on the power consumption of nodes in the network [19], and how to make movements in order to have the best state for the network lifetime.

1. Wireless sensor network lifetime definition

Based on previous researches, definition of the network lifetime depends on demands of different applications, such as the time when the network loses connection, the time when a certain percentage of the number of network nodes to consume their power capacity, or the time when coverage of wireless signal reduces to certain percentage. In our study, we define the network lifetime as the time when one of the nodes first enters into dead condition.

The sensor networks used in this study are mesh networks. The base station

can be located at the intersection of an arbitrary lattice. In the network nodes communicate with their four neighbors. If the information generated by the sensor nodes can not be directly transmitted to the base station, it will be transferred to the base station through multi-hops. When the sensor nodes and the base station are on the same horizontal or vertical line, the data will be able to send at the shortest path (straight line), otherwise there exist multiple data transmission paths to reach the base station. Each node in the network has the same data generation rate, and to calculate the network lifetime the sum of the retention time in the vicinity of the base station is used.

Parameters used in the Formula are listed in Table 2. When the base station location is at node *k*, the energy consumption of node *i* is calculated by Equation 1. Equation 2 represents power consumption of direct communication with the base station when the base station is in node i. To calculate the best staying time t_k of the base station at each location, a linear model is used. The best staying time is zero if the base station does not move to that location. Equation 3 represents the optimal stay time of base station at node *k*. Equation 4 gives the time limit. No specific rules are used to regulate the order for the base station to move into any node on the network, as long as power consumption on the nodes is balanced, it will work.

$$c_i^k = e\left(\sum_{j \in S_i} f_{ij}^k + \sum_{j:i \in S_j} f_{ji}^k\right), \qquad i, k \in N \text{ and } i \neq k \tag{1}$$

$$c_i^k = \square r, \qquad i, k \in N \text{ and } i = k \tag{2}$$

$$\text{Max } z = \sum_{k \in N} t_k \tag{3}$$

$$\text{such that } \sum_{k \in N} c_i^k t_k \leq \epsilon_0 \tag{4}$$

Table 2: The Symbol used in Equation 1 to Equation 4

Symbol	definition
ϵ_0	Initial energy of each node (Joules)
$\square$	Energy consumption coefficient of transmitting and receiving one bit (Joules/bit)
N	Numbers of sensor nodes
r	Data packets be generated at each nodes (bits/sec)
f_{ij}^k	Data transmission rate from node i to node j when base station at node k (bits/sec)
c_i^k	Power consumption at node i when base station stays at node k (Joules/sec)
t_k	Staying time of base station at node k (Seconds)
z	Network lifetime (Seconds)

To estimate the overall consumption of electricity, the location of the base station is taken as the base and the network is divided into eight areas, including: area to the left (HL), to the right (HR), above (VA) , below (VB), to the upper left (UL), to the upper right (UR), to the lower left (LL), and to the lower right (LR) of the base station, and Equation 5 to 12 were used to calculate energy consumption.

$$c_i^k = er[(x+1)(1+L)-1], \quad i \in HL \tag{5}$$

$$c_i^k = er[(L-x)(1+L)-1], \quad i \in HR \tag{6}$$

$$c_i^k = er[(y+1)(1+L)-1], \quad i \in VA \tag{7}$$

$$c_i^k = er(1+x+y), \quad i \in UL \tag{8}$$

$$c_i^k = er(L-x+y), \quad i \in UR \tag{9}$$

$$c_i^k = er(L+x-y), \quad i \in LL \tag{10}$$

$$c_i^k = er(2L-x-y-1), \quad i \in LR \tag{11}$$

$$c_i^k = er, \quad i = k \tag{12}$$

Simulations were performed to calculate the best staying time for the base station at each location according to above formula. The network has 8x8 nodes, and each node is initially charged to 1.35J. The data generation rate is set as 1 bit per second.

The optimal staying times of the base station in 8x8 networks are shown in Figure. 14. The row and column represent the location of nodes. Z. Maria Wang believed that if the base station stay according to the optimal time of each position, not only the node energy will be used with high effectiveness, but also the network lifetime will be maximized.

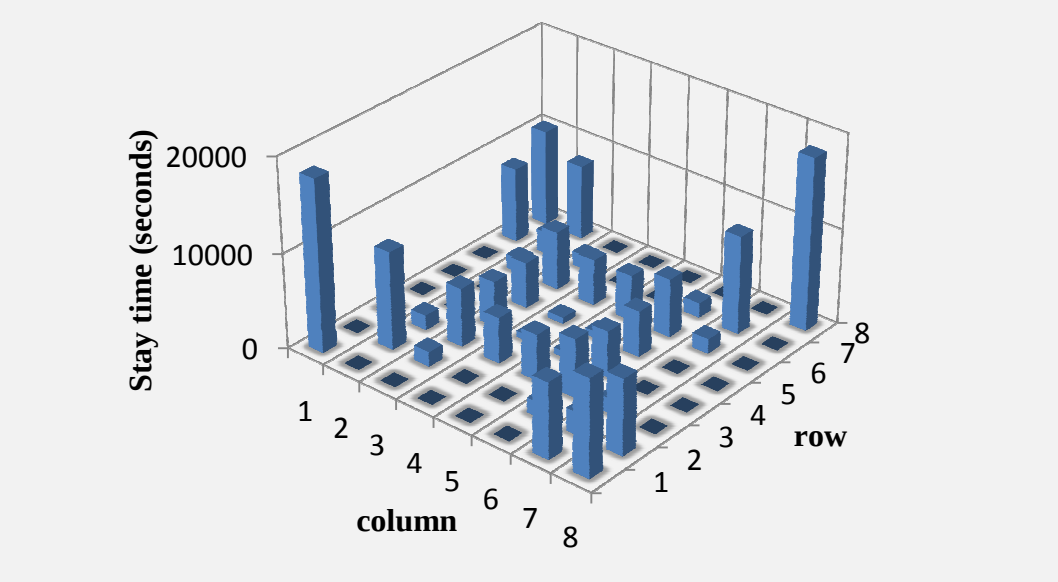


Figure 14: The optimal stay time of base station for 8x8 networks

Chapter 3 The proposed mobile base station scheme

3.1 The definition of anonymity

To increase anonymity of the base station and networks lifetime, a mobile base station scheme is proposed in this study. In wireless sensor network, the base station plays a major role. In order to protect identity of the base station, we will discuss the characteristics of the wireless network first.

There are two privacy-related definitions about the base station. We can achieve high security based on these two privacy-related definitions and prevent the base station from attacks.

1. Location anonymity

   The location of the base station and event nodes must be protected from disclosure. If the enemy knows the location of the event node that senses sensitive information or the location of the base station is tracked, he can destroy them very easily.

2. Role anonymity

   Any device in wireless sensor networks has its role. The general nodes need to monitor, sense environment, and forward information to the base station and they act as event nodes and nodes to forward information. The role of the base station was responsible to collect information. Once the base station is

destroyed, wireless sensor networks become useless. So, the base station is the most important in wireless sensor networks.

3.2 Model for quantifying anonymity of base station

In wireless sensor networks, many nodes are deployed in a wide region to detect information and monitor the environment. When an enemy wants to find out location of the base station through nodes, he can divide networks into several squared cells to facilitate analysis. In the following, we will discuss how to find the base station by analyzing traffic from the enemy's viewpoint.

3.2.1 Mathematical model of entropy

The entropy method is popular for estimating anonymity of the network. In 1948, Shannon proposed the information theory with a mathematical model for analyzing anonymity of a system. The model is used to measure randomness. In 2002, researchers used entropy to measure anonymity. In the anonymity measurement, the entropy shows how distributive the network traffic is. An enemy can divide networks into N cells and begin analyzing through his sensing area. After a period of time, he gives each cell a probability p_i which is the possibility of the base station appearing in cell *i*, then he can get a entropy value *H(x)* by the following equation [23]:

$$H(x) = -\sum_{i=0}^{N-1} [p_i * \log_2(p_i)] \qquad (13)$$

Initially, the probability of each cell is *1/N*, so the maximum entropy (p_i*=1/N*) is found to be $H_M(x)$ as follows [23]:

$$\mathrm{H_M(x)} = -\sum_{\mathrm{i=0}}^{\mathrm{N-1}} [\frac{1}{\mathrm{N}} * \log_2(\frac{1}{\mathrm{N}})] = \log_2 \mathrm{N} \qquad (14)$$

In order to estimate the anonymity, we calculate a ratio degree by Equation 15, in the paper we consider the ratio degree as the anonymity of base station.

$$\text{ratio degree} = \frac{\mathrm{H(x)}}{\mathrm{H_M(x)}} \qquad (15)$$

3.2.2 Estimating the anonymity of base station by entropy model

In this paper, we consider a global enemy who can eavesdrop the whole network to infer the location of the base station from packets transmitted to each cell. After observing the networks for a period of time, the enemy can compute the total transmitted packets, *T*, of the whole networks, and the number of packets, *Pi*, transmitted from cell *i*. The anonymity of the base station is calculated by Equation 16 and Equation 17.

$$\mathrm{H(x)} = -\sum_{\mathrm{i=0}}^{\mathrm{N-1}} \frac{\mathrm{P_i}}{\mathrm{T}} * [\log_2(\frac{\mathrm{P_i}}{\mathrm{T}})] \qquad (16)$$

$$\frac{H(x)}{H_M(x)} = \frac{-\sum_{i=0}^{N-1} \frac{P_i}{T} * [\log_2(\frac{P_i}{T})]}{\log_2 N} \quad (17)$$

3.3 Increasing the anonymity of base station by movement

When the wireless sensor network has been operating for a while, the enemy gathers enough information to predict the location of the base station. In this paper, we assume that the enemy can compute the number of transmitted packets by eavesdropping. If the base station is fixed, the enemy will quickly figure out the location of the base station because the traffic volume is high in vicinity of it. Therefore, we believe that periodically re-location of the base station will help reducing the probability of finding the base station. In addition, the remote enemy cannot detect the direction of the moving trajectory of the base station. So the method of the mobile base station can be used to reduce the possibility of discovery by the enemy.

3.3.1 What time to move base station?

First of all, we need to decide what time to move the base station. In order to avoid moving the base station too frequently and resulting in a high packet loss rate, we periodically re-locate the base station just as needed. When the time the base station decides to move, the best nest location has been decided and the

nodes in networks will stop transmitting. So we need to synchronize the time in all devices of networks.

3.3.2 What location will be selected by base station?

3.3.2.1 The assumptions of system

When the base station ready to move, it need to determine the best next location. In order to have complete information of traffic flow, the base station must be aware of the following information:

- Source node of each packet
- packet routing Path
- Nodes still having energy

From the packet header, the base station can get some information of the source node. But without the information of the packet routing path, the base station cannot accurately estimate the number of packets generated from each cell inside each area on the network. Because the packets are relayed through many nodes, the routing path of same packet is more than one. Our method is applicable when the base station has full knowledge of the routing path of each node.

3.3.2.2 The procedure for base station to select the best new location

We assume that the base station has accurate information about the routing path of each packet just like the global enemy. According to compute packets generated from each cell *i*, numbers of packets of every cell is summed up to get the total number of packet transmission. We compute the probability *Pi* by Equation 18. The definitions of symbol in Equation 18 are shown in Table 3s. *Pi* shows the activity degree of each cell; a low probability means that the activity of the cell is low and so the enemy assume the base station not be that cell. Thus we move the base station to the cell with the lowest activity of traffic.

$$P_i = \frac{packets_i}{Total\ transmit\ pacekts} \tag{18}$$

Table 3: The Symbol definition for Equation 19

Symbol	Definition
P_i	The percentage of packet transmitted
i	Cell number
$packet_i$	The packets transmitted of nodes in cell i

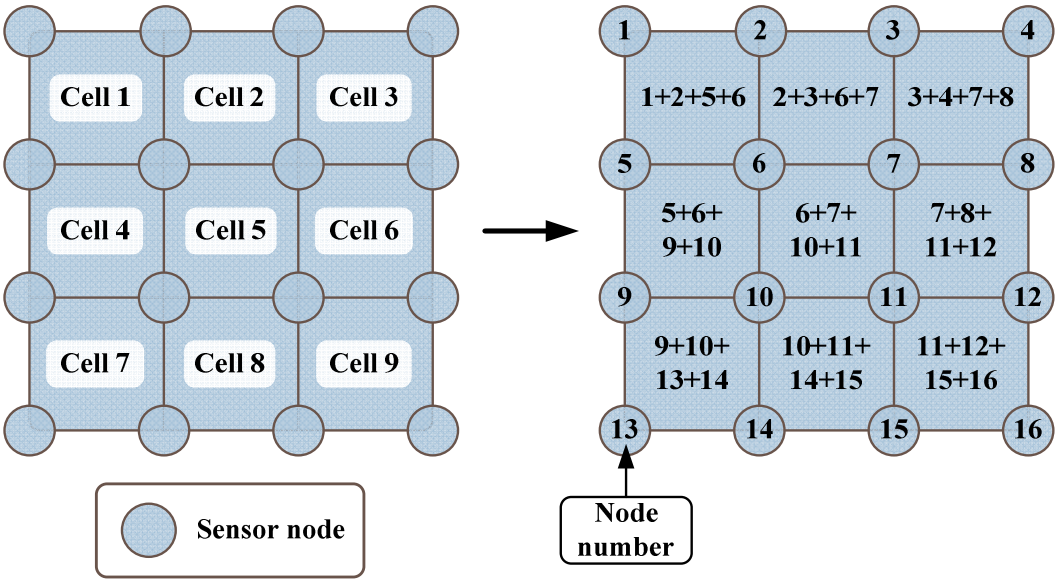


Figure 15: Estimating packets transmitted from each cell

Figure 15 shows how to calculate the number of packets generated in all cells. To compute the degree of activity of the nine cells, we sum up the number of generated packets of all nodes in the cell. For example the activity degree of cell 1 is calculated as the sum of the number of packets generated on node 1, 2, 5 and 6 divided by the total number of packets. When the base station has computed the degree of activity in each cell, it will select the location with the lowest degree of activity as the next location. Algorithm 1 shows the procedure that chooses an optimal area to move the base station.

Algorithm 1: The Algorithm of finding optimal area

Algorithm Find Optimal Area //Base station computes the optimal area to move. Input: The number of transmitted packets p_i's for $area_i$'s Output: The optimal area $area_i$ Integer packetAll, trafficOfArea[i], optimalArea, minTraffic; //Calculate the sum of packets with every area

```
for (i=0; i<number of area; i++)
      packetAll+=pi;
//Calculate the percentage of traffic volume with every area
for (i=0; i<number of area; i++)
      trafficOfArea[i]=pi/packetAll;
//Find the lowest traffic volume area
optimalArea=i;
minTraffic=trafficOfArea[0];
for (i=0; i<number of area; i++)
      if(minArea>trafficOfArea[i])
            optimalArea=i;
            minTraffic=trafficOfArea[i];
return optimalArea;
```

3.3.3 Moving and stopping the base station

Once the base station finds the location of the next cell according to the level of activity of each cell, it will move to the cell through a shortest path in order to resume normal operations of the network as fast as possible. In order to extend the network lifetime, after the base station selecting its next cell, it will choose a position, namely node i (the red colored base station in the figure) to stay based on remaining energy of nodes in the cell, as shown in Figure 16. The base station chooses node i since that node (blue color circles in the figure) has more energy than other nodes around it. In this way, we can distribute energy consumption by avoiding moving to a position with low energy levels.

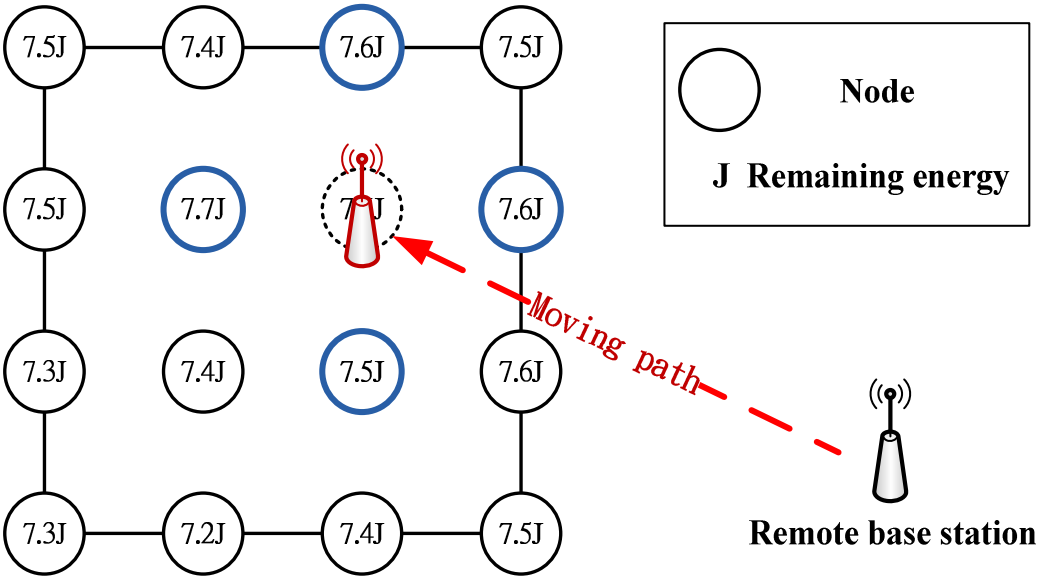


Figure 16: The diagram of selecting new BS location

Chapter 4 Experiments and simulation results

4.1 The setup of experiments

In this chapter we perform simulations of networks with the base station that can make movements, and compare the effect of the mobile base station. We divided networks into 3x3 and 5x5 cells with 100 and 256 sensor nodes, respectively. The base station initially locates at the center of the network, and the distribution of sensor nodes are as shown in Figure 17. In the experiments the events occur randomly, and 100 events are randomly generated every minute. Packets generated in events will be relayed to the base station by a unique shortest path with least hops, each packet size is set to 128 bytes. The initial power of each node is set to be 8 joules (J) [4], and the power consumptions for packet transmission and reception are equal. Substituting the packet size and power consumption into the formula, each packet sent or received will spend 0.000634 J. To investigate how the frequency of movements affects the security of the base station, the mobile base station makes movements at different time intervals of 30 minutes, 60 minutes and 90 minutes. In order to verify the ways of selection of the base station location will affect the network lifetime or not, the experiments employed two different location selecting approaches to determine the next location of base stations, namely random selected and residual energy based. In following figures, the “Energy” stands for our residual energy approach.

Table 4: The parameters of experiments

Parameters	Value
Network grid	3x3, 5x5 (cells)
Amount of nodes	100, 256 (nodes)
Number of nodes per cell	16 (nodes/cell)
Initial BS location	Central area
The way of events occur	Random
The freq. of events occur	100 (events/minute)
Routing path	Shortest path
Packet size	128 (bytes/packet)
Initial power of nodes	8J (Joules)
Power consumption of packet transmission and reception	0.000634J (Joules)
The freq. of BS movements	30, 60, 90 (minutes/times)

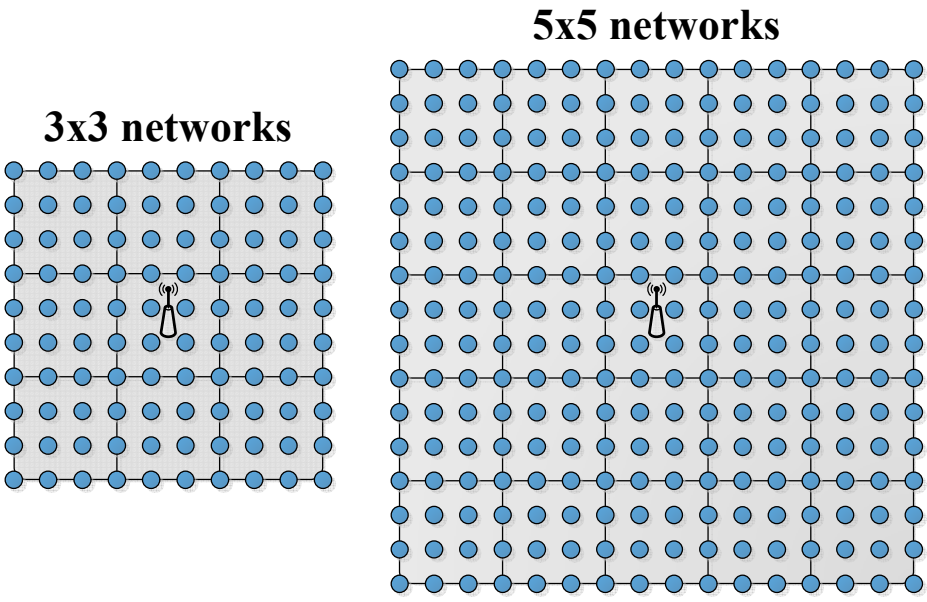


Figure 17: Deployments of WSNs for simulations

4.2 The experimental results

In this section we discuss the anonymity effect of the mobile base station over 3x3 and 5x5 network areas. The effects are observed for the following two criteria:

1. Anonymity

   In the experiments, whenever the base station decides to move, or a time interval of thirty minutes is reached, entropy of the network will be calculated and recorded to show the anonymity variation of the base station.

2. Network lifetime

   When any node in the network runs out of power, the number of generations of random events will be recorded. It can be used to evaluate how the ways of selection of the base station position and the movement frequency affect the networks lifetime.

4.2.1 The results of 3x3 areas

Figure 18 shows the anonymity of the base station fixed at central area of the 3x3 network. The anonymity decreases slowly over the time because the static base station leads to a higher traffic flow than the other areas. The way of event generation is randomly. The event does not occur in specific areas. Hence anonymity of the base station does not significantly decrease with the time.

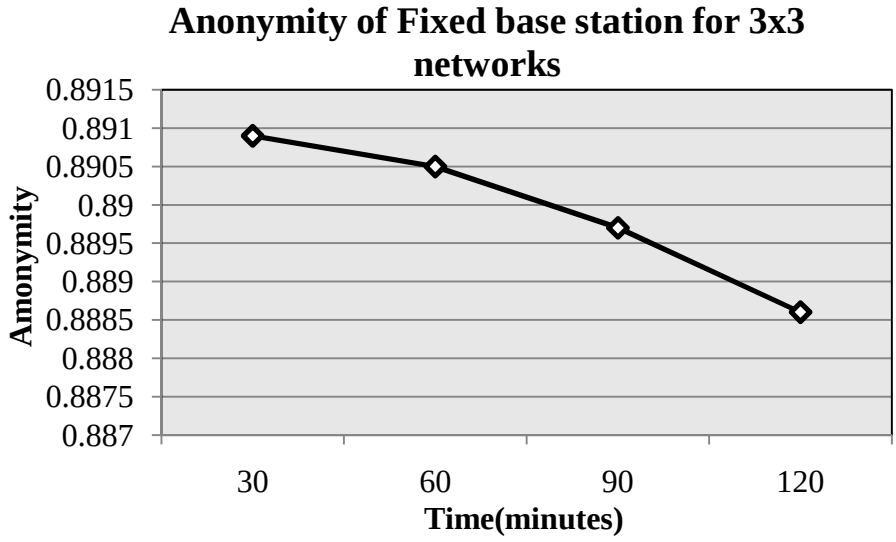


Figure 18: The anonymity of fixed base station in 3x3 networks

To evaluate the effect of our proposed method, we analyze the anonymity and network lifetime with following settings:

(1) Two methods of selecting the base station location: random selection and residue energy based.

(2) Different time interval: 30, 60, and 90 minutes between movements.

In Figure 19, Figure 20, and Figure 21, the y-axis represents the anonymity, and x-axis represents the time. The Figures show that the approach considering the remaining energy affects the base station anonymity more than random selection approach, because it can distribute traffic more evenly and the degree of anonymity is more than 0.99. However, both approaches can make enemies hard to find where the base station is. Figure 19 to 21 also show the effect of anonymity with different movement frequencies of the base station. If the base station moves more frequently, the anonymity will be enhanced. In Figure 22,

there are no data in the third and fourth movements (correspond to 270 and 360 minutes) because the network had nodes running out of energy and so the experiments were terminated accordingly.

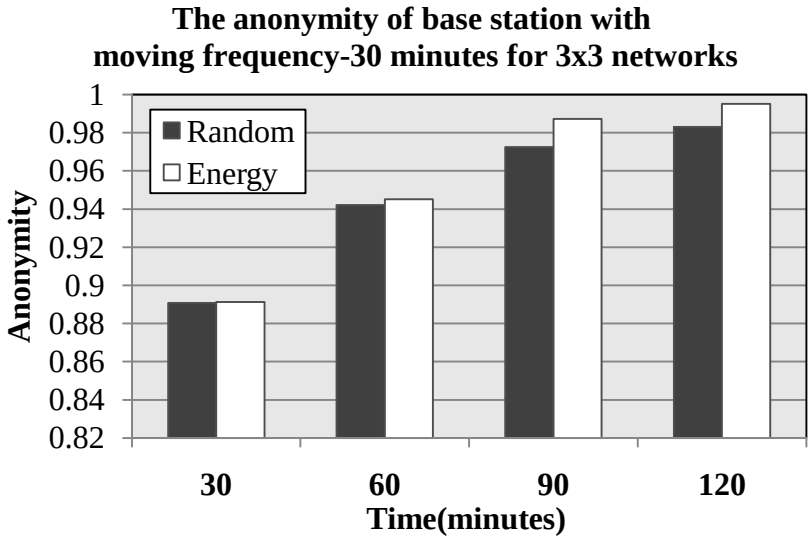


Figure19: The base station anonymity with moving frequency of 30 minutes for 3x3 networks

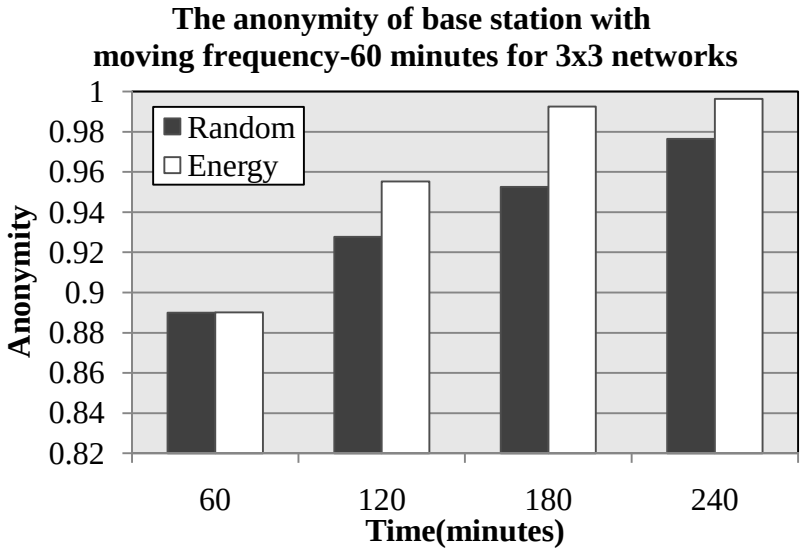


Figure 20: The base station anonymity with moving frequency of 60 minutes for 3x3 networks

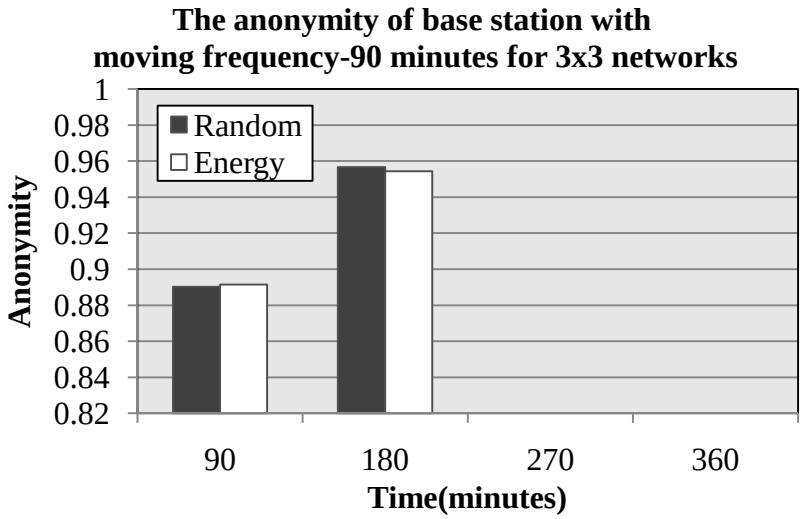


Figure 21: The base station anonymity with moving frequency of 90 minutes for 3x3 networks

Figure 22, Figure 23, and Figure 24 show how the two base station movement approaches affect the network lifetime. The time when some node in the network runs out of energy is defined as the network lifetime. These figures show that when location of the base station is fixed, at least one node will run out of energy after 12701 events are randomly generated in the network. From Figure 22, in which the mobile base station is moved in every 30 minutes, we observe that the residue power based approach has more network lifetime (by 42%) compared to the random selection approach. In Figure 22, the network lifetime of energy based approach is 3.96 times of the fixed base station approach; and 1.42 times of the random selection approach. In Figure 23, the base station is moved in every 60 minutes. The energy based approach improves the network lifetime to 2.75 times than the fixed base station approach, and 1.2 times than the random selection approach. In Figure 24, the base station is moved in every 90 minutes. The energy based approach improves network lifetime to 2.19 times than the fixed

base station approach, and 1.25 times than the random selection approach.

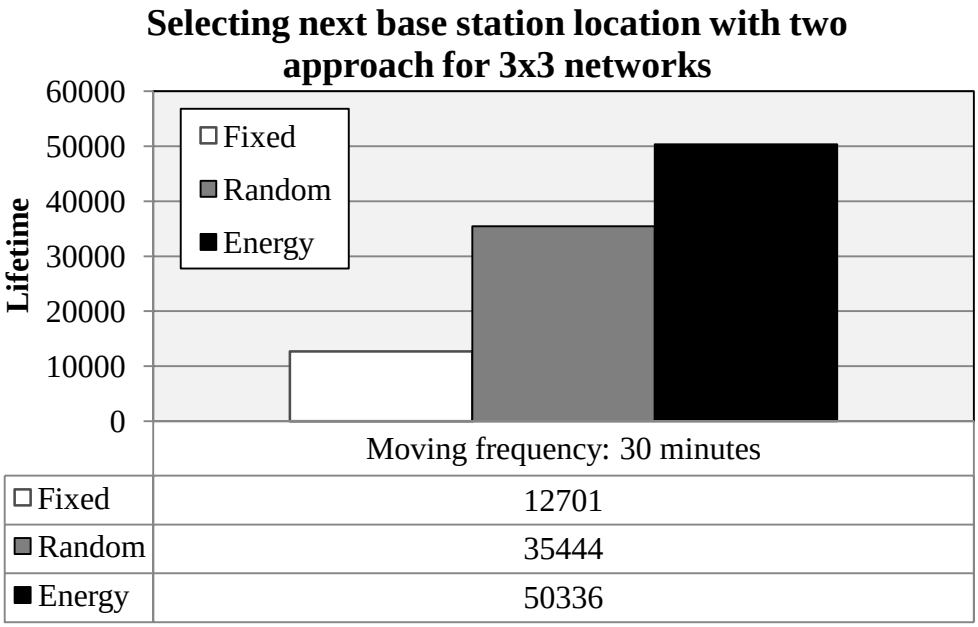


Figure 22: The network lifetime when the base station moves in every 30 minute in 3x3 networks

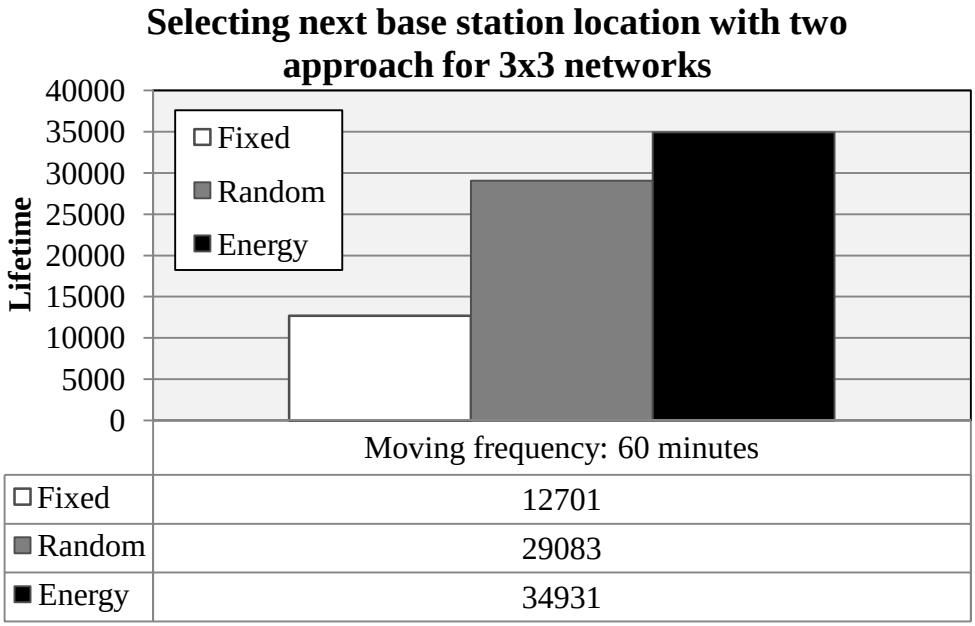


Figure 23: The network lifetime when the base station moves in every 60 minute in 3x3 networks

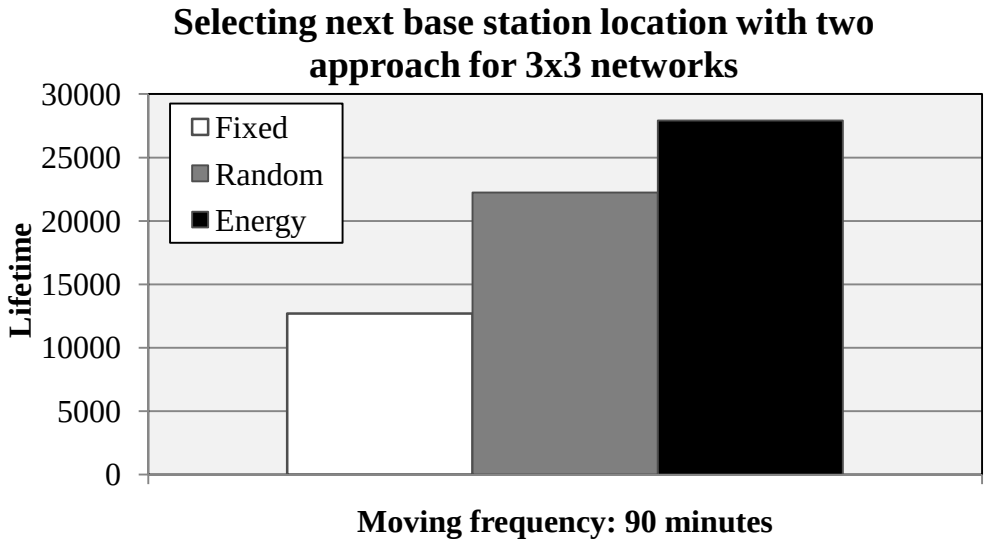
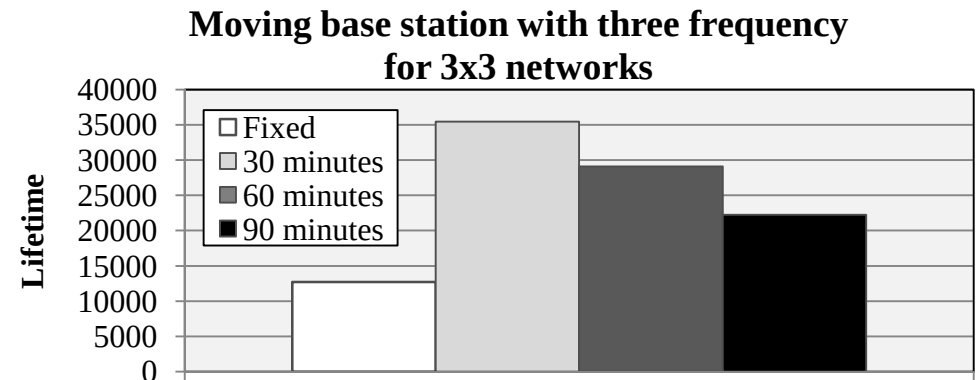


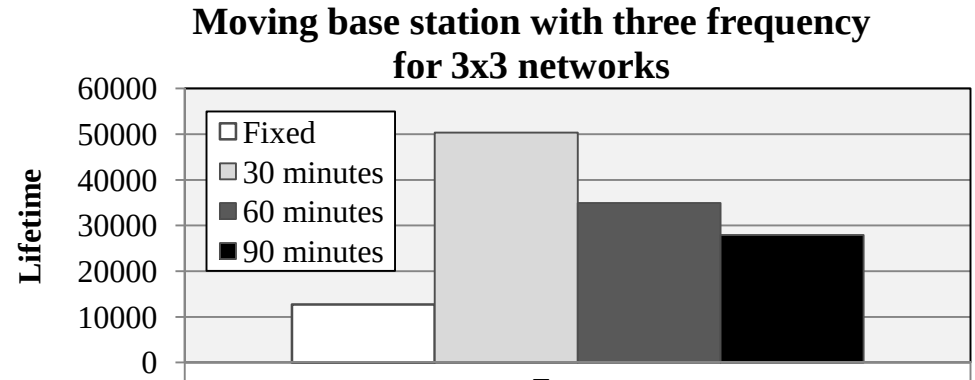
Figure 24: The network lifetime when the base station moves in every 90 minute in 3x3 networks

Figure 25 and Figure 26 show the impact on the network lifetime when the base station is moved in three different frequencies: in every 30, 60, and 90 minutes, respectively. We observe that when time interval becomes longer, the effect on the network lifetime becomes less. Figure 25 shows that the network lifetime when the base station is moved in every 30 minutes is 2.79 times, moved in every 60 minutes is 2.28 times, and moved in every 90 minutes is 1.75 times than that of the fixed base station. Figure 26 shows the same trend that the lifetime of moving the base station in every 30, 60, 90 minutes is 3.96, 2.75, and 2.19 times longer than the fixed base station approach. Thus, we may include that our energy based base station location approach is able to distribute traffic and balance the energy consumption of each node and prolong the lifetime of the network.



	Random
Fixed	12701
30 minutes	35444
60 minutes	29083
90 minutes	22235

Figure 25: Network lifetime with random selecting base station location for 3x3 networks



	Energy
Fixed	12701
30 minutes	50336
60 minutes	34931
90 minutes	27909

Figure 26: Network lifetime with our proposed method for 3x3 networks

4.2.2 The results of 5x5 WSN

The experimental results of 5x5 WSN are given here. Figure 27 shows that the results of experiments using randomly generated events. The result does not look like 3x3 WSN in the last section. The anonymity of the fixed base station decreases slowly but may suddenly increase later and it does not decrease substantially. One may argue that since the area of 5x5 networks are larger than that of 3x3 WSN, so the event occurs more randomly.

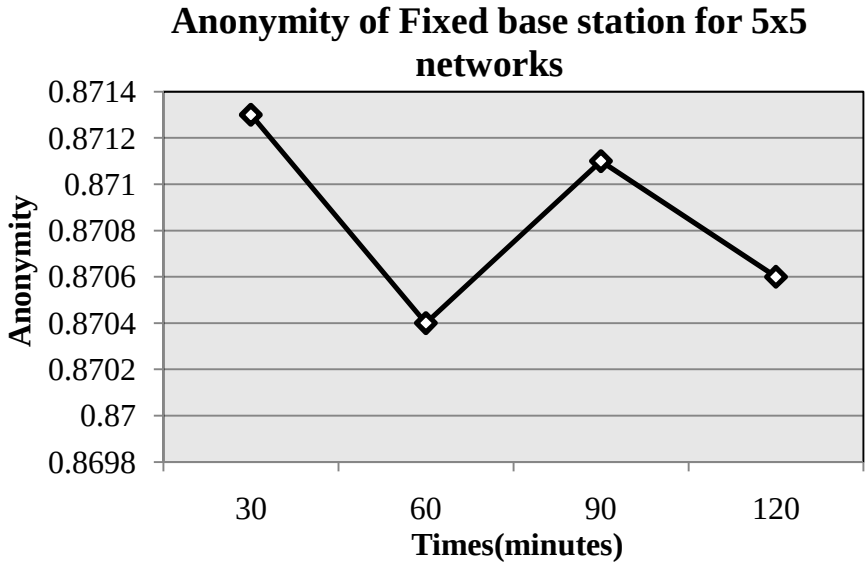


Figure 27: The anonymity of fixed base station in 5x5 networks

From Figure 28 to Figure 30 show the effect on anonymity of two location selection approaches for the base station in 5x5 networks. We observe that the anonymity increases when the number of movement increases and the two location selection approaches have similar effect on anonymity. In addition, we observe that the anonymity will increase quickly if the base station is moved more

frequently.

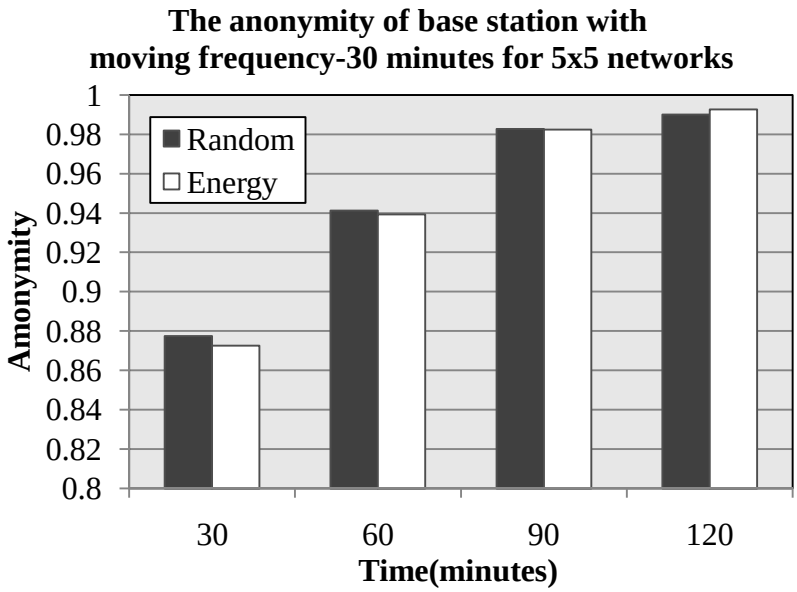


Figure 28: The base station anonymity with moving frequency-30 minutes for 5x5 networks

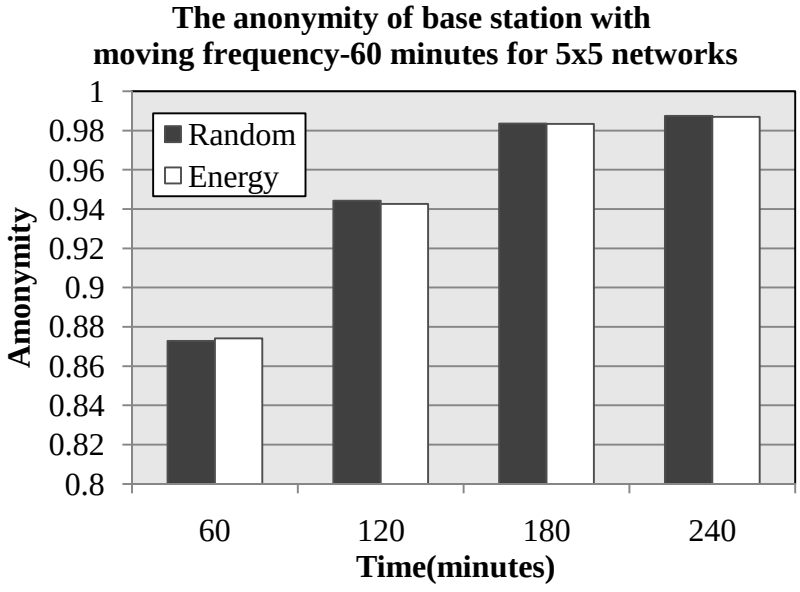


Figure 29: The base station anonymity with moving frequency-60 minutes for 5x5 networks

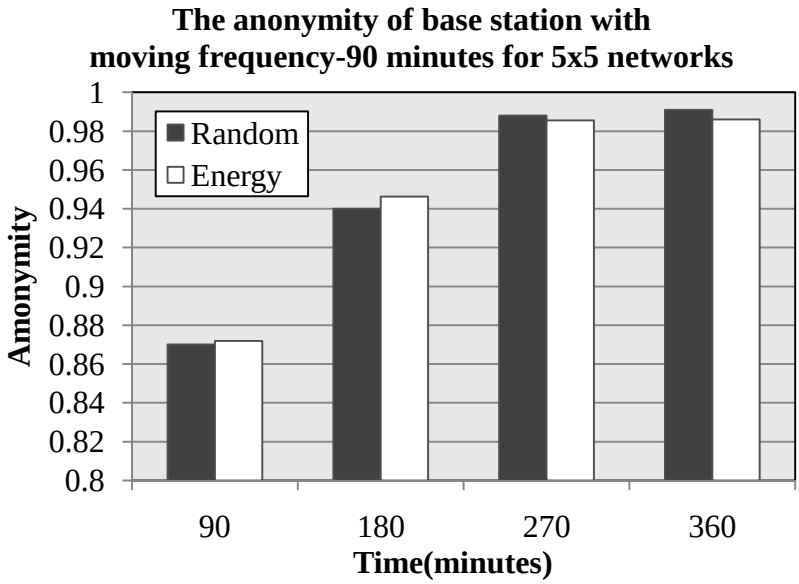


Figure 30: The base station anonymity with moving frequency-90 minutes for 5x5 networks

From Figure 31 to Figure 33 show effect on the network lifetime when the interval between movements of the base station is 30, 60, and 90 minutes. These figures show that when the base station is fixed, at least one node will run out of energy after 12626 events generated in the network. In Figure 31, mobile base station is moved in every 30 minutes, and we observe that the energy based location selection approach has 43% more network lifetime than the random selection approach. Furthermore, Figure 31 shows that the network lifetime for the energy based approach is 4.55 times of the fixed base station approach, and 1.43 times of the random selection approach. In Figure 32, the base station is moved in every 60 minutes, and the energy based approach improves the network lifetime to 3.77 times of the fixed base station approach, and 1.43 times of the random selection approach. In Figure 33, the base station is moved in every 90 minutes, and the energy based approach improves the network lifetime to 2.65

times of the fixed base station approach, and 1.47 times of the random selection approach.

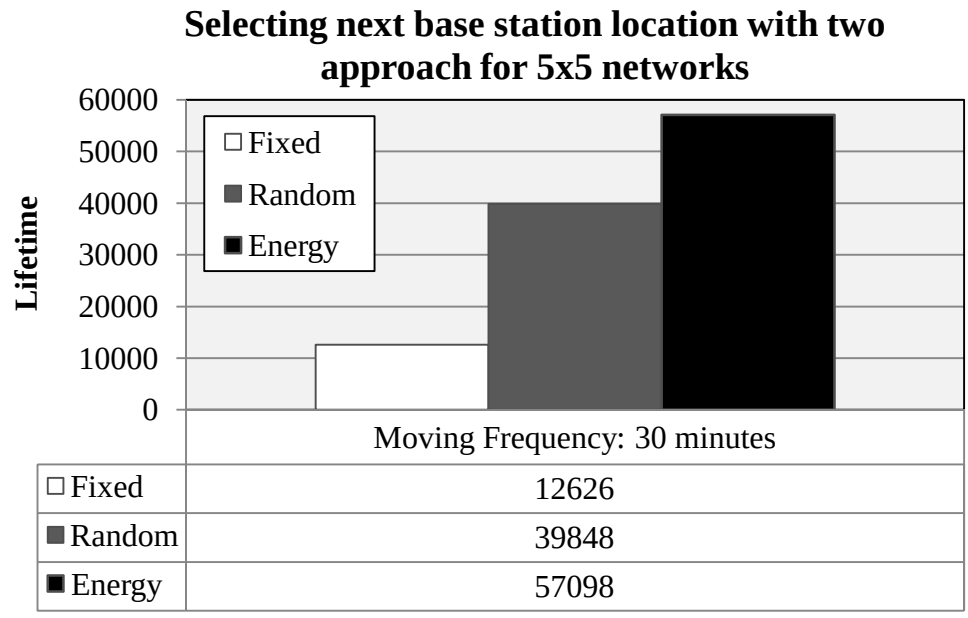


Figure 31: The network lifetime of moving base station every 30 minutes for 5x5 networks

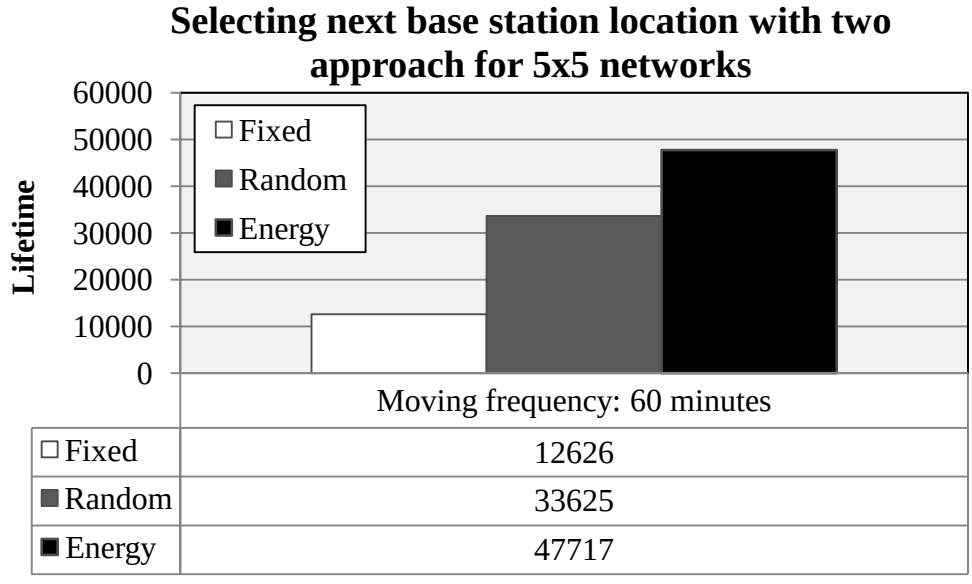


Figure 32: The network lifetime of moving base station every 60 minutes for 5x5 networks

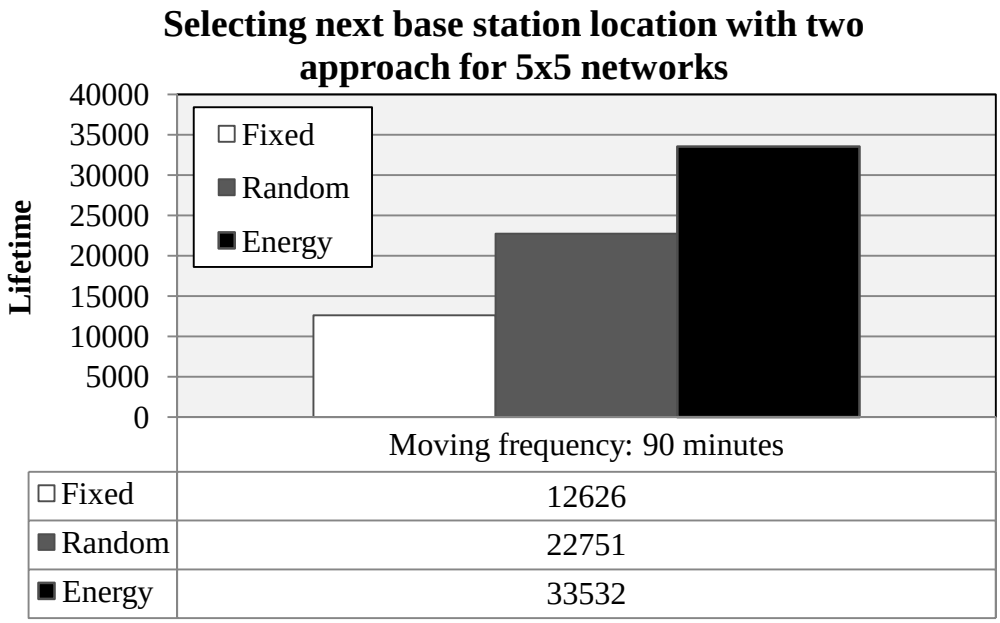


Figure 33: The network lifetime of moving base station every 90 minutes for 5x5 networks

Figure 34 and Figure 35 show the effect on the network lifetime when the base station is moved in three different frequencies. In Figure 34, the new location of the base station is selected randomly, and in Figure 35, is energy based. We observe that when the time interval of movement is increased, the increase of the network lifetime is reduced. Figure 34 shows that the network lifetime with the base station moved in every 30 minutes is 3.15 times than that with a fixed base station, 1.18 times than that with the base station moved in every 60 minutes, and 1.75 times than that with the base station moved in every 90 minutes. Figure 35 shows that the network lifetime with the base station moved in every 30 minutes is 4.52 times than that with a fixed base station, 1.19 times than that with the base station moved in every 60 minutes, and 1.70 times than that with the base station moved in every 90 minutes. We conclude that our proposed energy based method

is able to distribute traffic and balance the energy consumption of nodes, so the anonymity of the base station is enhanced and the network lifetime is prolonged.

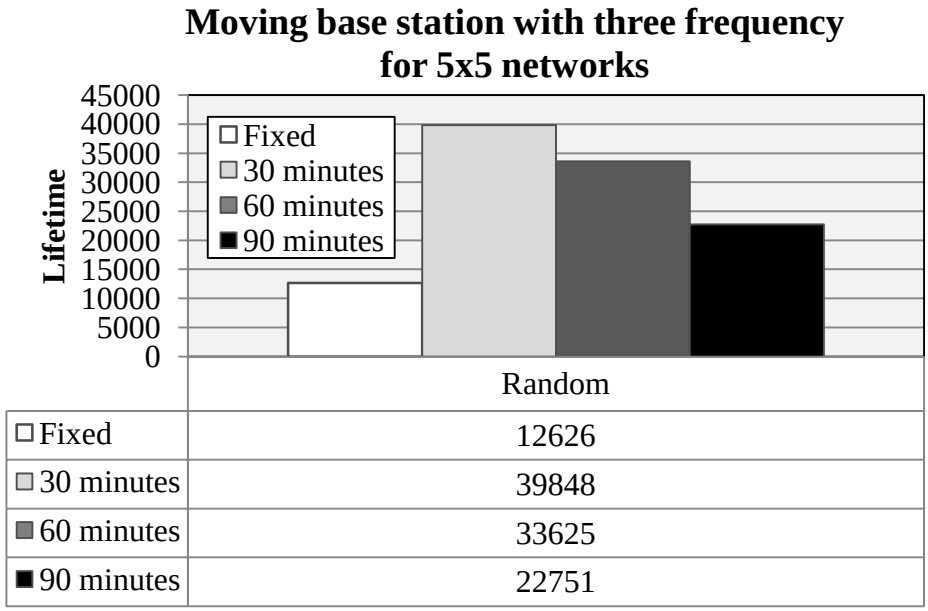


Figure 34: Network lifetime with random selecting base station location for 5x5 networks

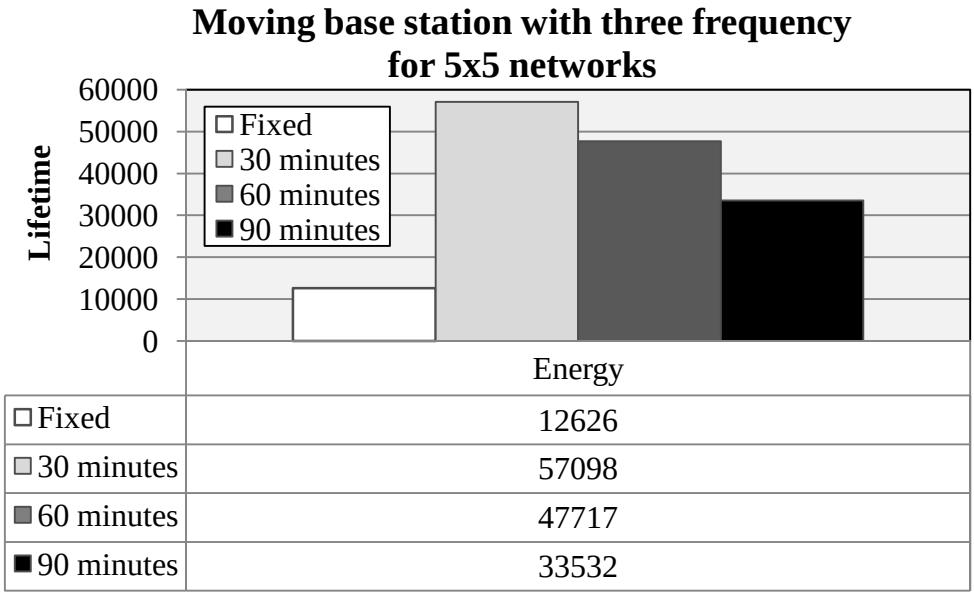


Figure 35: Network lifetime with our proposed method for 5x5 networks

The longest network lifetime of three different moving frequencies for the 5x5 network are 57,098, 47,717 and 33,532; while the longest network lifetime for the 3x3 network are 50,336, 34,931, and 27,909, respectively. The experimental results show that when the network is larger, it is more effective to extend the network lifetime by the mobile base station scheme.

Chapter 5 Conclusions

The base station plays the most important role in wireless sensor networks. It collects information for any node in the network and then sends the collected information to the host computer for further processing. If the base station does not work properly, the whole wireless sensor network will lose its function. Therefore, the base station is the major target for enemies. The goal of this research is to reduce the enemy's probability of finding the base station, and we have proposed a residue energy based approach to implement a mobile base station to enhance to anonymity and prolong the network lifetime.

The simulation results prove that our mobile base station can effectively increase the entropy of the network. If the mobile base station is moved more frequently, the entropy will be higher. The entropy is similar using the residue energy approach alone and using the random selection approach plus the lowest probability area scheme. When the network area is divided to more grids, the energy selection approach of the mobile base station will benefit more. Compared with the fixed base station, the network lifetime of the mobile station approach is extended at least two folds. The experimental results also reveal that in the larger network of 5×5, the lifetime of network is extended at least four folds. Therefore, the larger the network is, the more benefit obtained by using the proposed approach.

Although moving the base station increases the anonymity of the base station and prolongs the lifetime of the network, some problems are induced, for example,

since nodes in the network cannot communicate with the base station while the base station is moving, some packets are lost. A better routing approach is called for to solve this problem and prevent the loss of packets, and this could be one of the worthiest themes for the future work.

Bibliography

[1] Paolo Barontib, Prashant Pillaia, Vince W.C. Chooka, Stefano Chessab, Alberto Gottab, and Y. Fun Hu, “Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards,” *Computer Communications*, vol.30, no.7, May. 2007, pp. 1655-1695.

[2] Na Li, Nan Zhang, Sajal K. Das, and Bhavani Thuraisingham, “Privacy preservation in wireless sensor networks: A state-of-the-art survey,” *Ad Hoc Networks*, vol. 7, 2009, pp. 1501-1514.

[3] Yun Zhou, Yuguang Fang and Yanchao Zhang, “Securing wireless sensor networks: A survey,” *IEEE Communications*, vol. 10, no. 3, 2008, pp. 6-28.

[4] Uday Archarya, Mohamed Younis, “Increasing base-station anonymity in wireless sensor networks,” *Ad Hoc Networks*, vol. 8, 2010, pp. 791-809.

[5] Jing Deng, Richard Han, and Shivakant Mishra, “Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks,” *Elsevier Pervasive and Mobile Computing Journal*, vol.2, no.2, Apr. 2006, pp. 159-186.

[6] Alireza A. Nezhad, Ali Miri, and Dimitris Makrakis, “Location privacy and anonymity preserving routing for wireless sensor networks,” *Computer Networks*, vol.52, 2008, pp. 3433-3452.

[7] Haodong Wang, Bo Sheng, and Qun Li, “Privacy-aware routing in sensor networks,” *Computer Networks*, vol. 53, 2009, pp. 1512-1529.

[8] A. Pfitzmann, M. Hansen, “A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability,

pseudonymity, and identity management," *Working draft. Anon Terminology v0.34*, Aug. 2010.

[9] J. Deng, R. Han, and S. Mishra, "Enhancing base station security in wireless sensor networks," *Technical Report CU-CS951-03, Department of Computer Science, Univ. of Colorado*, Apr. 2003.

[10] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," *Security and Privacy for Emerging Areas in Communication Networks*, Sep. 2005.

[11] Y. Jian, S.G. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," *Computer Communications*, May. 2007, pp. 1955-1963.

[12] Stefano Basagni, Alessio Carosi, Emanuel Melachrinoudis, Chiara Petrioli, and Z. Maria Wang "Controlled sink mobility for prolonging wireless sensor networks lifetime," *Wireless Networks*, vol.14, 2008, pp. 831-858.

[13] Yinying Yang, Mirela I. Fonoage, and Mihaela Cardei "Improving network lifetime with mobile wireless sensor networks," *Computer Communications*, vol. 33, 2010, pp. 409-419.

[14] Young Sang Yun, Ye Xia, "Maximizing the lifetime of wireless sensor networks with mobile sink in delay-tolerant applications," *IEEE Transactions on mobile computing*, vol. 9, no. 9, Sep. 2010.

[15] Jun Luo, Jacques Panchard, Micha Pi´orkowski, Matthias Grossglauser, and Jean-Pierre Hubaux. "MobiRoute: Routing towards a mobile sink for improving lifetime in sensor networks," *Distributed Computing in Sensor Systems*, San Francisco. USA, Jun. 2006, pp. 480-497.

[16] Mirela Marta, Mihaela Cardei, “Using sink mobility to increase wireless sensor networks lifetime,” *World of Wireless, Mobile and Multimedia Networks,* California USA, Jun. 2008, pp.1-10.

[17] Yanzhong Bi, Jianwei Niu, Limin Sun, Wei Huangfu, and Yi Sun, “Moving schemes for mobile sinks in wireless sensor networks,” *IEEE International Performance, Computing, and Communications Conference,* Los Angeles, USA, Apr. 2007, pp. 101-108.

[18] Tao Yang, Makoto Ikeda, Gjergji Mino, Leonard Barolli, Arjan Durresi, and Fatos Xhafa, “Performance evaluation of wireless sensor networks for mobile sink considering consumed energy metric,” *IEEE International Conference on Advanced Information Networking and Applications Workshops,* Perth. Australia, Apr. 2010.

[19] Z. Maria Wang, Stefano Basagni, Emanuel Melachrinoudis, and Chiara Petriili, “Exploiting sink mobility for maximizing sensor networks lifetime,” *Hawaii International Conference on In System Sciences,* Hawaii. USA, Jan. 2005.

[20] Manoj K. Joshi, Lawrence Osborne, Bo Sun, and S. Kami Makki, “Hot spot aware energy efficient clustering approach for Wireless Sensor Networks,” *IEEE Consumer Communications and Networking Conference,* Las Vegas. USA, Jan. 2011, pp.585-589.

[21] R. C. Shah, S. Roy, S. Jain, and W. Brunette, “Data MULEs: Modeling a three-tier architecture for sparse sensor networks,” *IEEE International Workshop on Sensor Network Protocols and Applications,* May. 2003, pp. 30-41.

[22] H. S. Kim, T. F. Abdelzaher, and W. H. Kwon, “Minimum energy asynchronous dissemination to mobile sinks in wireless sensor networks,” *Embedded Networked Sensor Systems*, Los Angeles. USA, Nov. 2003, pp. 193-204.

[23] C. E. SHANNON, “A mathematical theory of communication,” *The Bell System Technical Journal*, vol. 27, pp. 623-656, Oct. 1948, pp. 379-423.

[24] B. Selman, H. Levesque, and D. Mitchell. “A new method for solving hard satisfiability problems,” *National Conference on Artificial Intelligence*, CA. USA, July. 1992, pp. 440-446.