A KEY DISTRIBUTION SCHEME FOR MOBILE UNDERWATER WIRELESS SENSOR NETWORKS

by
KÜBRA KALKAN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
June 2011

A KEY DISTRIBUTION SCHEME FOR MOBILE UNDERWATER WIRELESS SENSOR NETWORKS

APPROVED BY

Assoc. Prof. Dr. Albert Levi .....

(Thesis Supervisor)

Assoc. Prof. Dr. Erkay Savaş .....

Assist. Prof. Dr. Cemal Yılmaz .....

Asst. Prof. Dr. Hüsnü Yenigün .....

Assoc. Prof. Dr. Özgür Erçetin .....

DATE OF APPROVAL .....

A KEY DISTRIBUTION SCHEME FOR MOBILE UNDERWATER WIRELESS SENSOR NETWORKS

Kübra Kalkan
Computer Science and Engineering, MS Thesis, 2011
Thesis Supervisor: Assoc. Prof. Albert Levi
Keywords: Underwater Sensor Networks, Security, Key Distribution

Abstract

Wireless Sensor Networks consist of small battery-limited devices called sensor nodes. They are used for collecting data from surrounding environment and relay them via wireless communication. One of the recent application areas is underwater sensing. Communication in Underwater Wireless Sensor Networks (UWSN) is different from airborne communication. Radio frequencies cannot be used for UWSN. Instead acoustic waves, which cause extra challenges, are used in UWSN. When UWSNs are deployed in hostile environment, nodes can be captured by an adversary. In order to secure UWSNs, firstly key distribution problem must be addressed. Moreover, UWSNs are inherently mobile since the nodes may be drifted in the sea.

In this thesis, we propose a key distribution model which is applied for two group mobility models, namely (i) nomadic mobility model and (ii) meandering current mobility model. Our nomadic mobility based key distribution scheme works in three dimensions. However, this scheme is suitable only for small coastal areas. On the other hand, our meandering mobility based key distribution model is a two dimensional one and spans several kilometers in the open sea. In both schemes, a hierarchical structure is used. Secure and resilient group communication is handled via well-known Blom's key distribution scheme. We analyzed the performance of the proposed schemes using simulations. Our results show that secure connectivity of both schemes is generally high. Of course, mobility causes some temporary decreases in the connectivity, but our schemes help to heal the connectivity performance in time. Moreover, our schemes show good resiliency performance such that capture of some nodes by an adversary only causes very small amount of links between uncaptured nodes to be compromised.

SUALTI HAREKETLİ KABLOSUZ DUYARGA AĞLARI İÇİN BİR ANAHTAR DAĞITIM YÖNTEMİ

Kübra Kalkan
Bilgisayar Bilimi ve Mühendisliği, Yüksek Lisans Tezi, 2011
Tez Danışmanı: Doç. Dr. Albert Levi
Anahtar Kelimeler: Sualtı Duyarga Ağları, Güvenlik, Anahtar Dağıtımı.

Özet

Kablosuz Duyarga Ağları, duyarga düğümleri adı verilen sınırlı bataryaya sahip küçük aygıtlardan oluşur. Kendi çevrelerinden veri toplamak ve bu verileri kablosuz iletişimle dağıtmak için kullanılırlar. Son zamanlardaki uygulama alanlarından biri sualtı algılamasıdır. Sualtı Kablosuz Duyarga Ağları (SKDA)'nda iletişim hava yoluyla iletişimden farklıdır. SKDA'lar için radyo frekansları kullanılamaz. Bunun yerine, SKDA'larda, ekstra zorluğa sebep olan akustik dalgalar kullanılır. SKDA'lar saldırıya açık bir alana dağıtıldıklarında, düğümler saldırgan tarafından ele geçirilebilir. SDKA'larda güvenliği sağlayabilmek için anahtar dağılım problemi çözülmelidir. Ayrıca, SDKA'lar denizde sürüklenebileceklerinden dolayı hareketlidirler.

Bu tezde, (i) göçebe hareket modeli ve (ii) kıvrımlı akıntı hareket modeli; isimli iki grup hareket modeli için uygulanabilen bir anahtar dağılım modeli önerilmiştir. Göçebe hareket modeline dayalı anahtar dağılım şemamız üç boyutta çalışabilmektedir. Ancak, bu şema ancak küçük kıyı alanlar için uygundur. Diğer yandan, kıvrımlı akıntı hareket modeline dayalı anahtar dağılım şemamız iki boyutlu ve açık denizde kilometrelerce alana yayılabilmektedir. Her iki şemada da hiyerarşik bir yapı kullanılmıştır. Güvenli ve dayanıklı grup iletişimi, yaygın olarak bilinen Blom anahtar dağılım şeması yardımı ile sağlandı. Önerilen şemaların performanslarını simülasyon kullanarak analiz ettik. Sonuçlarımız iki şemanın da güvenli bağlanılabilirliği genellikle yüksek çıktığını göstermiştir. Elbette; hareketlilik, bağlanılabilirlikte bazı geçici düşüşlere sebep olabilir. Ancak şemalarımızın yapısı, zaman içinde bağlanılabilirlik performansının iyileşmesine yardımcı olmaktadır. Dahası şemalarımız, bazı düğümlerin düşman tarafından ele geçmesinin ele geçirilmemiş düğümler arasındaki

bağların çok az miktarının öğrenilmesine sebep olduğu güzel bir dayanıklılık performansı göstermektedir.

Acknowledgements

I would like to thank my thesis supervisor, Assoc. Prof. Albert Levi, for all his support throughout my undergraduate and graduate education and for guiding me in my studies.

I also thank Assoc. Prof. Erkay Savaş, Asst. Prof. Dr. Cemal Yılmaz, Asst. Prof. Dr. Hüsnü Yenigün and Assoc. Prof. Özgür Erçetin for devoting their time to join my jury despite their busy schedule.

I thank my beautiful family for supporting me in every aspects of my life and growing me up to this day without any pay-back.

I specially thank my love Hakan Çakmakci for being there whenever I need him.

During my graduate education, I was supported by scholarships of Sabancı University and Scientific and Technological Research Council of Turkey (TÜBİTAK). I am grateful to these foundations for supporting my education.

Table of Contents

List of Figures

Chapter 1

Introduction

Wireless sensor networks which consist of small battery powered devices are applied in various applications such as military, agriculture, habitat monitoring and healthcare [1,24]. Another application area of wireless sensor networks is underwater aquatic applications which recently attract network research community [6, 35, 36, 37, 38, 48]. These networks are used for military underwater surveillance, oceanographic data collection, ecology, public safety and industrial products [33].

In underwater conditions, communication is not as easy as airborne. Radio frequency which is used for airborne wireless communication, is not suitable for underwater. For that reason acoustic frequency has to be used in communication which results in some challenges.[37, 46, 47] Acoustic communication has large latency, low bandwidth and high error-rate which have to be considered in underwater modeling [6]. As Underwater Wireless Sensor Network (UWSN) is a recent area, mostly main problems are addressed by researchers such as synchronization [40], data gathering

[39], localization [41], routing protocols [42,43], energy minimization and MAC issues [44,45]. Despite the fact that underwater networks are in a hostile environment which are suitable for node capture attacks, there is not much research on security of UWSN. In this thesis, we work on security in UWSNs.

Security for networks is provided by cryptographic mechanisms such as encryption and decryption operations. However these operations are not trivial for sensor networks, since sensor devices have limited memory and computational power. In addition, transmission in underwater networks is more energy consuming process because of acoustic frequencies.

There are two types of encryption/decryption operations: Public Key Cryptography and Symmetric Key Cryptography. In public key cryptography, each user has its own private and public keys. Sender encrypts message by using receiver's public key. Then receiver decrypts the message by using its own private key. This operation requires too much energy which is not suitable for sensor networks. In symmetric key both sides have the same key for encryption/decryption operations. This operation is more suitable for wireless sensor network since it does not consume large amount of energy. However, in symmetric key cryptography it is not trivial to distribute those secret keys.

There are various key distribution mechanisms that are proposed for wireless sensor networks. One of the main mechanisms is Basic Scheme of Eschanuer and Gligor [16]. This scheme provides a trade-off between connectivity of sensors and resiliency of the network against capture attacks. There are also hierarchical types of key distribution mechanisms which have clusters of normal sensors and cluster heads that communicate with the main station [27, 28, 29]. This reduces the communication in the whole network. As in underwater networks transmission is costly, it is important to reduce the communication. Hence, hierarchical networks are more suitable for underwater sensor networks. There is also another type of mechanism called Blom's scheme which is based on matrices [20]. This scheme has λ security, which means that network is resilient until λ nodes are captured. In our scheme we have also utilized from Blom's scheme to increase resiliency of the network.

In addition to security issue, mobility is another issue in underwater. There are several factors such as current and underwater living creatures that drift nodes.

Therefore underwater network models should be designed by considering mobility of nodes. There are some entity and group mobility models for sensor networks. One of the main entity models is random walk mobility model [29]. There are also other mobility models such as random way point mobility model, random direction mobility model, Gauss-Markov mobility model etc. Some of the group mobility models are nomadic mobility, column mobility model, pursue mobility model and reference point group mobility models [29]. As nodes are drifted by the affect of similar sources, nodes move in groups. For this reason, group mobility models are more suitable for underwater sensor networks. In addition, there is a mobility model called meandering current mobility model that is based on ocean dynamics which drifts nodes via currents.

1.1 Our Motivation and Contribution of the Thesis

As underwater sensor network is a recent research area, there is not enough work on security issues since fundamental challenges are focused initially. Especially there is no proposed scheme for key distribution. In this thesis, we proposed two key distribution models for underwater wireless sensor networks.

In underwater network, all models must be designed by considering mobility issue. In this thesis, we propose two key distribution models based on two mobility models. In the first model, nodes move in view of nomadic mobility model. Nomadic Mobility Key Distribution Model is a three dimensional model for small areas. Other key distribution model is based on Meandering Current Mobility Model. This model is applicable for large areas but it is a two dimensional model. For both models, we perform performance analysis to measure connectivity and resiliency. Both schemes have nearly perfect resiliency since Blom's scheme is utilized in groups. Adversary cannot compromise any additional links using the nodes he/she captured previously. Connectivity is also around 1.0 since it is recovered by the help of elevator model.

1.2 Organization of the Thesis

The remainder of this thesis is organized as follows: Chapter 2 gives preliminary information about underwater wireless sensor networks and its challenges, network structure types for sensor networks, security and key distribution background. This chapter also includes explanation of Blom's scheme and background information about mobility models. In Chapter 3, we explained about our scheme Nomadic Mobility

Based Key Distribution Model and show its performance. In Chapter 4, we introduced our model called Meandering Current Mobility Based Key Distribution Model and give its results. Finally Chapter 5 concludes the thesis.

Chapter 2

Background Information

2.1 Underwater Wireless Sensor Networks (UWSNs)

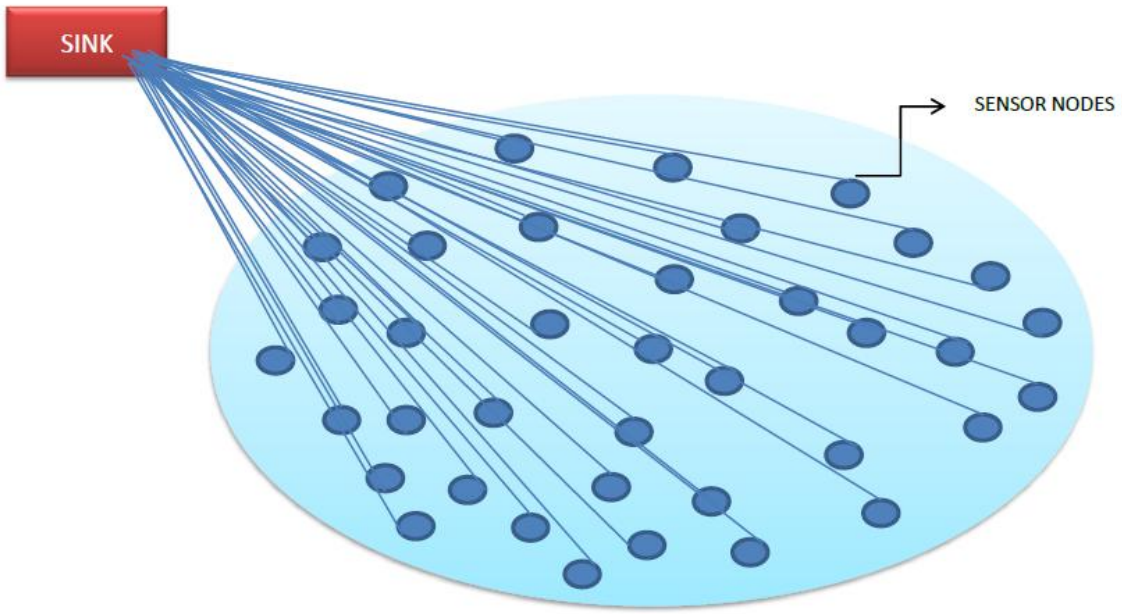
Wireless sensor networks (WSNs), consist of small, inexpensive devices called *sensor nodes* [1]. Sensor nodes have limited battery, memory, data processing capacity and short transmission range. They can measure different types of physical properties such as temperature, sound, pressure etc [2]. They can track an object or monitor the surrounding environment to collect data [1, 3, 4, 5]. They have a wide range of application areas such as health-care monitoring, military applications, agriculture and habitat monitoring. Also recently there is a growing interest in monitoring aqueous environments such as rivers, oceans and lakes for scientific and commercial aims [6].

Since the physical properties of air and acoustic environment is different, sensing needs special type of network which are called underwater sensor networks.

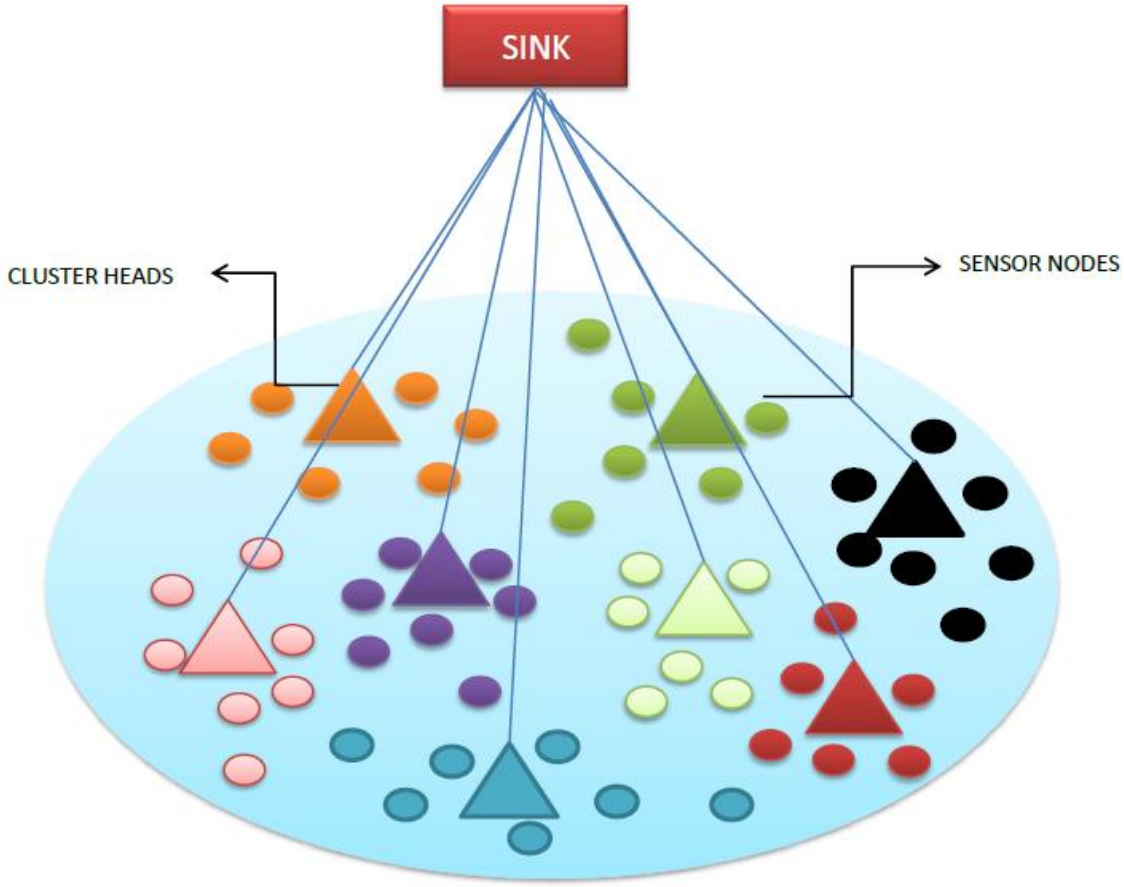
Due to the communication system in underwater, there are lots of challenges in underwater sensor network modeling. Communication system is more difficult in underwater conditions than airborne communication. This implies that usage of terrestrial WSN is not possible for UWSN [7]. Since radio frequency does not work well in underwater, in UWSN nodes should communicate using acoustic frequency. Acoustic communication has large latency, low bandwidth and high error-rate [6]. In addition, as there are currents in acoustic environments, nodes are dragged with water which adds a mobility aspect to the problem. Also, underwater environment is not suitable for human exploration because of high pressure, unpredictable underwater activities and vast size of water area [7]. Due to all those difficulties, modeling in underwater sensor networks requires much more effort to come up with those challenges.

2.2 Network Structure

There are different types of wireless sensor networks according to their network structure. They can be hierarchical or distributed (flat) as it can be seen in Figure 2.1. In distributed network all sensor nodes communicate with the main station called *sink*, and also they can communicate with the nodes which are in their range. All nodes have equal power and there is no hierarchy for their communication. On the other hand, in hierarchical network, there are clusters of nodes where nodes from different clusters communicate via the heads of clusters [2, 12, 13, 14].



(a)



(b)

Figure 2.1 (a) Flat Network Structure (b) Hierarchical Network Structure

Radio frequencies do not work well in underwater sensor networks. For this reason, technologies like GPS, which are used to control the location of nodes, cannot be used in underwater. Therefore, in most localization schemes some reference nodes are used. These reference nodes' places are known and they are used to determine other nodes' position by calculating their distance according to the reference nodes [15]. This fact leads to construct the structure in a hierarchical way. In this structure, some nodes are special ones. These are called *anchor nodes* and they are used as reference points. In addition as it will be explained in Section 2.3, hierarchical structure is more suitable for key distribution in underwater sensor networks. Since acoustic frequencies, which consume huge amount of energy, are used in underwater networks, it is important to reduce the communication. In hierarchical network design communication is decreased which makes it suitable for underwater sensor networks.

2.3 Security and Key Distribution Background

Underwater wireless sensor networks are deployed to hostile environment in which it is possible to capture nodes. Since networks can be used for military applications, it is significant to model the network resilient to attacks. Besides, sensor readings should be protected securely [8]. In a wireless application an adversary not only can eavesdrop the traffic but also can interrupt the messages [2]. As far as underwater sensor networks are wireless applications, security requirements for wireless sensor networks are also valid for underwater sensor networks. Some security requirements for wireless applications are data confidentiality, integrity, freshness, availability, self organization, time synchronization, secure localization and authentication [9].

Data confidentiality is the protection of data from unauthorized parties against eavesdropping. It is provided by encryption of the message with a secret key. Integrity is the assurance that the message received is exactly same as the message that is sent by the authorized party. In other words, if integrity is provided, then there is no insertion, deletion or modification in the message. Freshness suggests that the data is a recent message. That is to say it is the assurance that data is not a replay of an old message. Availability means that WSN can provide service whenever it is needed. Self

organization suggests that every node is independent and it can heal itself under several conditions. Most of the applications depend on a time concept which requires time synchronization between nodes. Secure localization is the ability to locate each nodes position automatically and accurately. Authentication is the assurance that the communicating entity is the one it claims to be.

Cryptographic mechanisms are used to handle authentication, data confidentiality and integrity problems. There are two types of cryptographic mechanisms for encryption: asymmetric key cryptography and symmetric key cryptography.

In symmetric key cryptography, there is one key which is used for both decryption and encryption. Sender encrypts the message using that common key and sends it to the other party. Then receiver decrypts message by using the same key. Main challenge in symmetric key is the distribution of this common key to the entities.

In an asymmetric key cryptography (a.k.a. public-key cryptography), each entity has its own public and private keys. Private key is only known by the owner; whereas, public key is known by anyone. Sender encrypts the message by using the public key of the sender. Then receiver decrypts the message by using his own private key. As no common keys are used in asymmetric cryptography, key distribution is trivial. However, public key operations require more energy and computational power. Due the limited battery of sensor nodes, public key cryptography is not preferred for wireless sensor networks; thus symmetric key is used for wireless sensor networks, similarly for underwater wireless sensor networks [10, 11].

Distribution of symmetric keys is not a trivial problem that many researchers have studied in this area and proposed lots of schemes [2, 16, 17, 18, 19, 20, 21]. It is not trivial since there is a trade-off between memory and resiliency. If only one pairwise key is used in whole network, it is obvious that if any of nodes is captured, adversary can compromise all nodes in the network, which means that network is not resilient to capture attacks. On the other hand, if different pairwise keys are generated for each pair, it is resilient to capture attacks since if a node is captured it cannot learn any information about other links. However, in this model each node should store $n-1$ keys, where n is the number of nodes in network. As nodes have limited memory, it is not possible for a node to store that much key information. Hence, it is not easy to handle resiliency and memory issues in key distribution.

First scheme about key distribution in wireless sensor network was proposed by Eschenauer and Gligor [16]. This scheme is also called as basic scheme and is based on random key pre-distribution. Each node is preloaded with keys from a key pool randomly before they are deployed. This phase is called key-predistribution phase. Then, the nodes are randomly deployed to the area, where each node starts the process to learn its neighbors. As the nodes have random keys, they may share common keys with its neighbors. Two nodes can communicate if they have common keys; otherwise, they cannot communicate directly. Looking for a common key process is called shared key discovery phase. If two neighbors do not have common keys, then they try to find a path to communicate via other direct links. This phase is also called path-key establishment phase. If the number of keys loaded to nodes is increased it is obvious that the probability of finding common keys will increase which means that connectivity of the entire network will also increase. However the main problem of this scheme is that when number of keys in memories of nodes increases, resiliency to attacks decreases. If a node is captured, adversary can easily reach other nodes' keys, which means that there is a security problem. Hence in basic scheme, if network is more connected then it is less secure.

Several other schemes are inspired from the basic scheme [17, 24, 25, 26]. Most of those schemes work in distributed fashion in which any two sensor nodes can establish pairwise keys. Due the fact that wireless sensor networks have large amount of nodes and high density, distributed structure leads to consume high amount of energy for key distribution. Moreover, their communication overhead is significant. In that sense, this is more serious for underwater sensor networks since acoustic waves, which consume more energy than radio frequencies, are used for underwater communication. Thus, hierarchical structures are more favorable than distributed ones for underwater wireless sensor networks. In that sense, we have also employed a hierarchical structure for our key distribution models.

As nodes have short transmission range, only neighboring nodes need to secure their communication; they do not need share common keys with far away nodes. Based on this idea, in hierarchical structure nodes in the same cluster communicate with each other. If a node needs to communicate with a node from another cluster, they can communicate via their cluster heads.

Jolly et al. proposed a scheme for hierarchical wireless sensor networks [28]. In this scheme, network is made up of clusters where each cluster has a gateway node

(cluster head) and several normal sensor nodes. Each node communicates only with its gateway node, and gateways can talk to each other and the sink. Each gateway node is loaded with several keys for normal nodes before deployment and each sensor is loaded with a gateway's ID and a key shared with this gateway. After deployment if sensor node's cluster head has the same ID with gateway ID in sensor node's memory, then this cluster head and sensor node establish a secure link. Otherwise, cluster head requests the desired key from corresponding gateway. Then, cluster head and sensor node can communicate securely. In this scheme, network performance is increased since hierarchical network is used. However, in this scheme resiliency problem is not addressed. If any gateway node is captured, all nodes' links which take their keys from this gateway are compromised. Also in this model, to increase the performance they use a group key for gateway's communication, which reduces security significantly. If a gateway node is captured, adversary can compromise all the communications among other gateways. Therefore, it is obvious that if a gateway node is captured, all network is crashed.

In our scheme, we used hierarchical network to increase network performance. However we used some techniques to handle the resiliency problem. The technique that we used in our scheme to increase security is Blom's scheme which is explained in details below.

2.4 Blom's Scheme

In random pool based schemes, there is not a guarantee that two neighbors share a common key which means that they need to communicate via other secure links that increases the communication overhead. Also this affects security of the network negatively. Blom proposed an approach which guarantees that any two nodes in a group can generate a common key [20]. This is a matrix-based solution. Also, it has λ-secure property where λ is a threshold. Network is secure until λ nodes are captured. If more than λ nodes are captured, all keys in the group are revealed.

In this scheme, initially public and private matrices are generated by a key distribution center. Let G be the public matrix such that any $(\lambda + 1)$ columns are linearly independent. It has the size of $(\lambda + 1)$ x N , where N is number of nodes in a

group and λ is an expected threshold. A well-known example of such matrix is a Van Der Monde matrix. It is in the following format:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ s & s^2 & s^3 & \cdots & s^N \\ s^2 & (s^2)^2 & (s^3)^2 & \cdots & (s^N)^2 \\ & & \vdots & & \\ s^\lambda & (s^2)^\lambda & (s^3)^\lambda & \cdots & (s^N)^\lambda \end{pmatrix} \quad \text{mod } q$$

When s is a primitive element of a prime $q > N$, the values s, s^2, s^3,…, s^N are all distinct which makes all columns of G linearly independent.

In Blom's scheme, there is also a private D matrix of size $(\lambda + 1)$x $(\lambda + 1)$ which is known to the key distribution center only. The transpose of $D.G$ is denoted by A. That is $A = DG^T$. The rows of A are private information own to each node. $K = A.G$ is the symmetric matrix which includes the pairwise keys. Each element $k_{ij} = k_{ji} \in K$ is the key shared between node i and node j.

Each node is loaded with a row of A such that node i is loaded with i^{th} row of A . There is no need to load public matrix to nodes memory, since it can be calculated if the seed s and q are known. For this reason, each node is only loaded with s and q. If node i wants to communicate with node j, then node i, calculates the j^{th} raw of matrix G and multiplies it with its own private information which is i^{th}row of A. As a result it finds k_{ij} which is element at i^{th} row and j^{th} column of K. Similarly, node j, calculates the i^{th} raw of matrix G and multiplies it j^{th} row of A and finds k_{ji} which is element at j^{th}row and i^{th} column of K. Since K is a symmetric matrix, $k_{ij} = k_{ji}$. All these matrices are depicted in Figure 2.2.

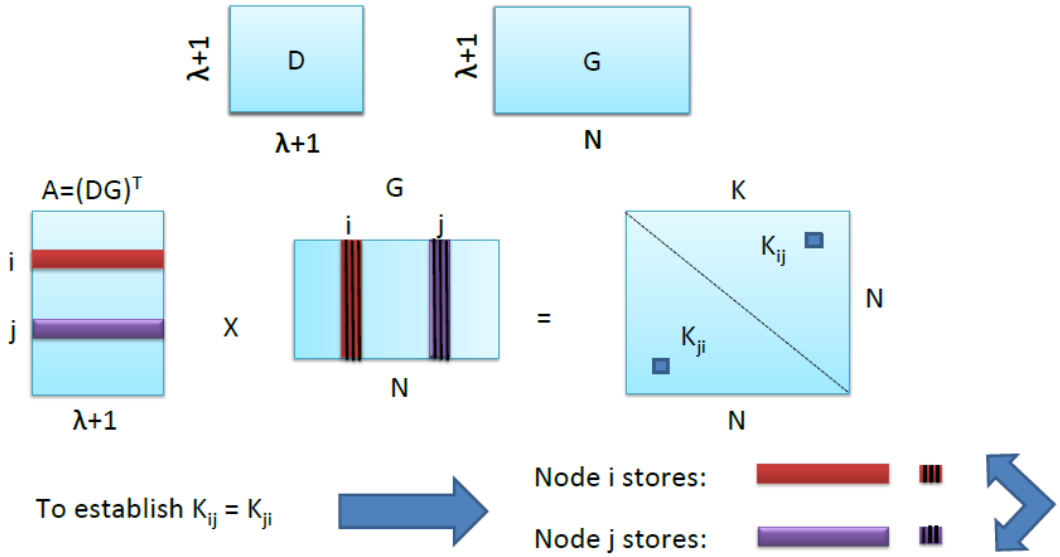


Figure 2.2 Blom's scheme

By combining Blom's scheme and basic scheme, Du et al. proposed an approach called Multiple Space Key Pre-distribution scheme [21]. In this model, there are multiple key spaces in the key pool. Nodes are pre-loaded with *h* different key spaces randomly. Then they are deployed to the environment. If two nodes have a common key material from same key space, then they can generate a Blom key, otherwise they try to generate a path-key via secure links. This scheme increases resiliency of Blom's scheme, however due to path-key establishment phase, communication and computational overhead increase. Also, nodes have to store more key spaces, which increase memory overhead. In underwater network, communication overhead is a significant issue. Thus, Multiple Space Key Pre-distribution scheme is not suitable for our scheme. We preferred to employ Blom's scheme for in our key distribution scheme.

2.5 Mobility Models

In underwater networks there are external factors such as current, wind and underwater creatures which drift nodes in the water. For that reason underwater networks should be modeled by considering their mobility. There are lots of mobility models for wireless sensor networks some of which are explained below.

Mobility models can be classified as entity mobility models and group mobility models. One of the main entity mobility models is Random Walk Mobility Model [29]. In this model each node moves with random speed to random direction. Nodes direction can be between [0,2π] and its speed can be between [minspeed, maxspeed] range where minspeed is the minimum speed and maxspeed is the maximum speed that each node can have. Each node travels a distance $d$with randomly chosen speed in constant time t. After a node reaches to the destination, it chooses another direction and speed randomly. When it reaches to a boundary of the area, it bounces off the border with an angle which is determined by the incoming direction. Many versions of Random Walk Mobility models exist such as 1-*D*, 2-*D*, 3-*D* and *d*-*D* walks. Since it does not use any past information about speed and direction, this model is known as memoryless model. Figure 2.3 shows the traveling pattern of a single node using Random Walk Mobility Model. There are also several entity models such as random way point mobility model, random direction mobility model, Gauss-Markov mobility model [29].

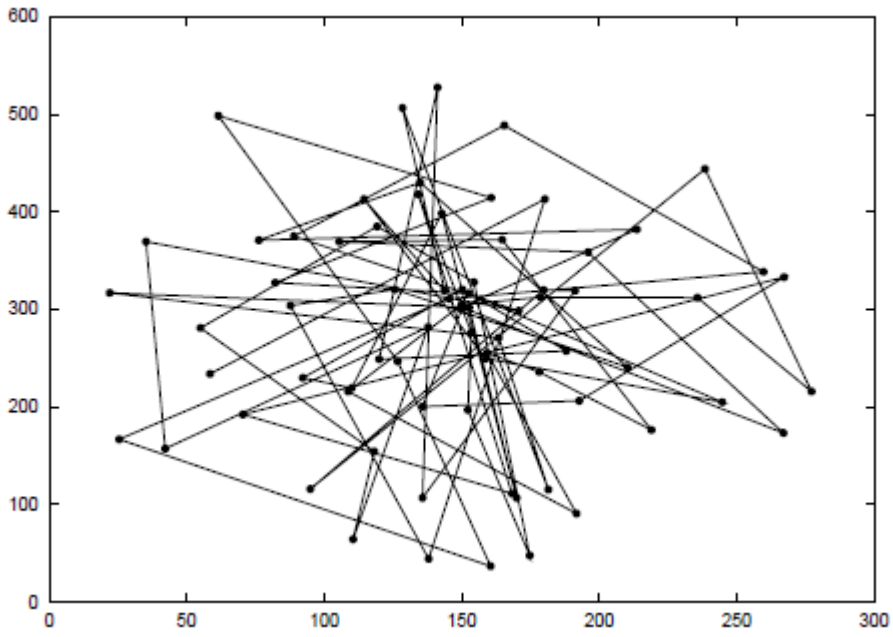


Figure 2.3 Traveling pattern of a single node using random walk mobility model [29]

There are also group mobility models which examine not only one node's mobility behavior but also all nodes mobility in network. Nomadic mobility is one of the well-known group based mobility models [29]. In this model, nodes act like an ancient nomadic community. Group moves from one reference point to another

collectively and individuals move randomly around this reference point. As all nodes move together to new reference point, they roam around the new reference point as shown in Figure 2.4. There are also several group mobility models such as column mobility model, pursue mobility model, reference point group mobility model etc.

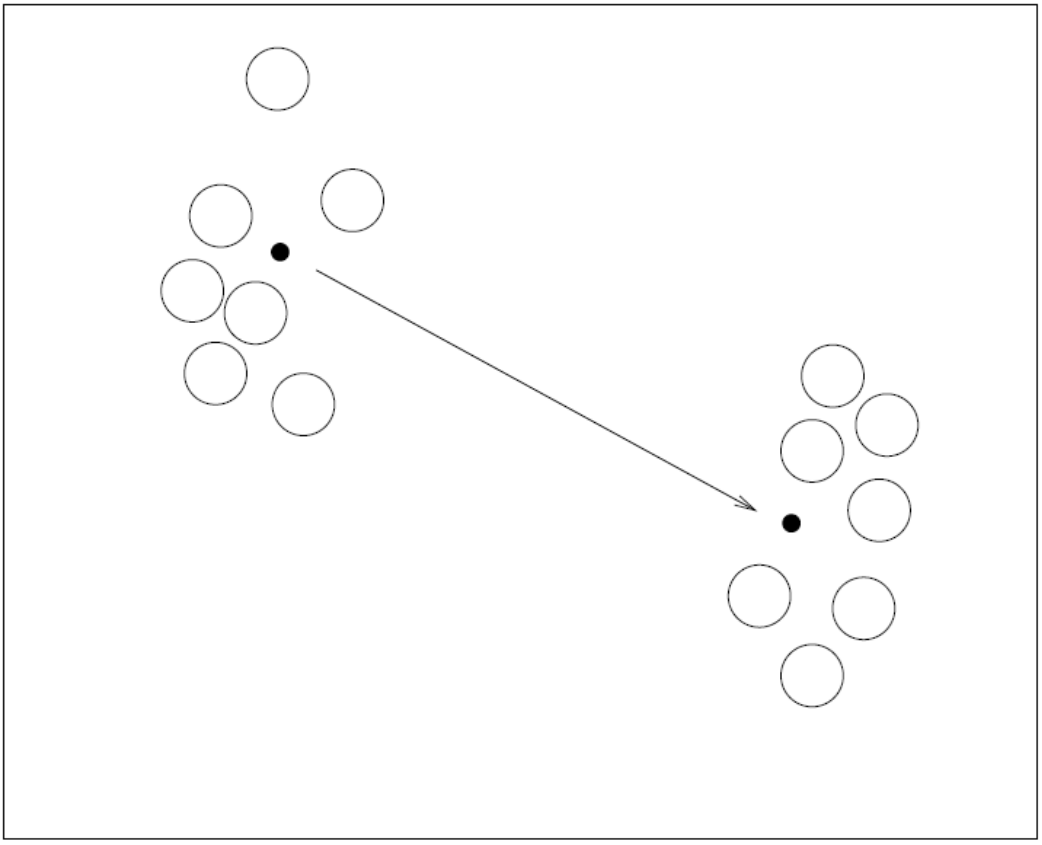


Figure 2.4 Movements of seven nodes using nomadic community model [29]

Each sensor moves independently from others in most of the mobility models for mobile sensor networks in the literature [30-32]. However in underwater network, nodes move with the effect of stream which means that it is important to propose a model which takes into account the dynamics of the water [33]. Nodes will be affected from similar forces which results in nodes' group mobility. To consider this issue, in our model we use nomadic community mobility model which is designed as nodes are drifted with a current in groups.

Caruso et al. proposed a mobility model for underwater sensor networks called Meandering Current Mobility model [33]. In this model, nodes are moving by the affect of meandering sub-surface currents and vortices. This model is for large ocean environments that span several kilometers. They consider that paths of nodes are

deterministic and there is a strong correlation between nearby sensors. In order to simulate nodes mobility, it is important to model the movement of ocean in which they are immersed. Vertical movements in ocean are negligible with respect to horizontal ones [34]. Thus, in their model they neglect vertical displacement which makes mobility in 2D. The details of the model are explained in Chapter 4.

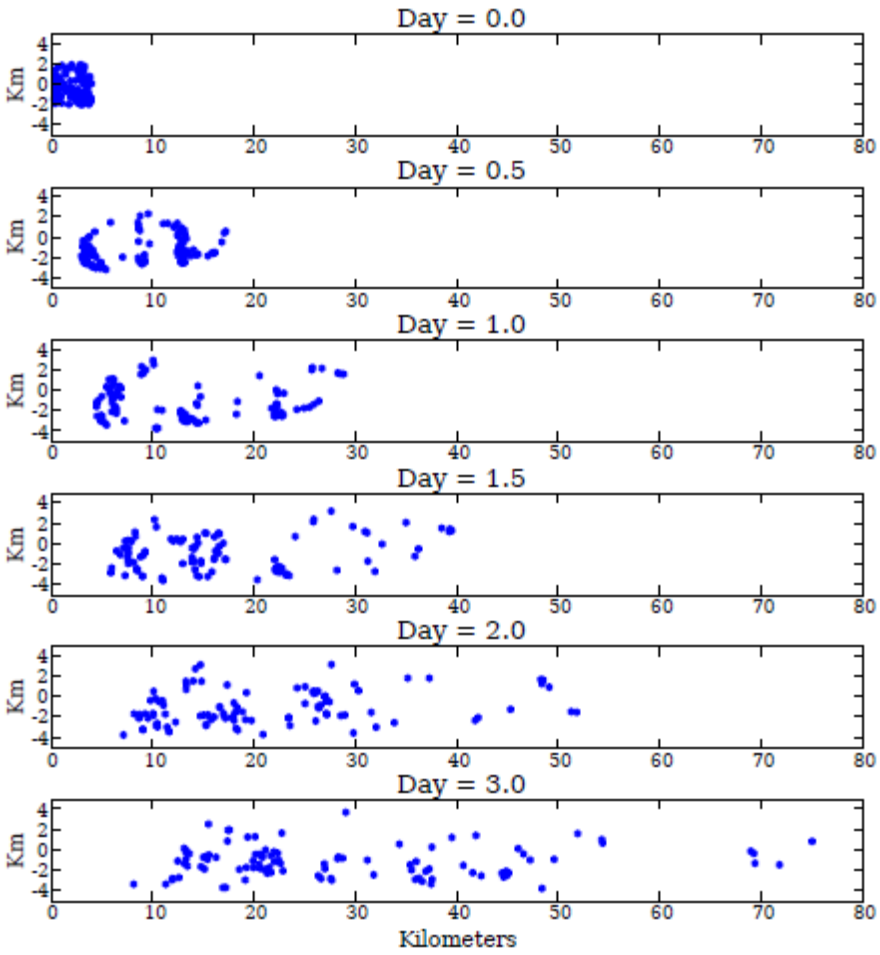


Figure 2.5 Time evolution of the position of one hundred sensors randomly released in a square of 4 km of side [33].

Movement of the nodes in 3 days is depicted in Figure 2.5. This model is more realistic than other group mobility models for WSNs since nodes are drifted according to the movement of the ocean. In this thesis, we also propose a security model which is based on Meandering Current Mobility Model.

Chapter 3

A Key Distribution Scheme for Underwater Sensor Networks with Nomadic Mobility Model

3.1 Network Architecture of Nomadic Mobility Based Model

In this work, our goal is to develop a key distribution model, which is applicable for underwater sensor networks. This model is designed as three dimensional model and it is a coastal model; in other words it is not for large areas like oceans. It is assumed that nodes do not go away from the designated area.

Key distribution in underwater sensor network is a challenging problem, since underwater communication is airborne communication. As mentioned in Section 2.2 and Section 2.3, hierarchical network, which reduces the communication cost of nodes, is more suitable for underwater sensor networks. Communication cost is tried to be lessened in underwater sensor networks because of the cost of acoustic frequencies.

Therefore, hierarchical network structure which decreases communication cost is more applicable for underwater sensor networks.

One of the hierarchical underwater sensor network schemes is proposed by Zhou et al [49]. The aim of this is scheme is to solve localization problem for underwater sensor network. This system consists of three types of nodes: surface buoys, anchor nodes and ordinary sensor nodes. Each surface buoy is equipped with GPSs. In this system, all the anchor nodes can estimate their positions by contacting directly with surface buoys. Ordinary nodes localization is also determined through anchor nodes. In another scheme [50], Dive and Rise (DNR) positioning is proposed. In this scheme, each DNR beacons are equipped with GPSs. Beacons are moving in y coordinate. When beacons come to the surface, they learn their places by the help of GPS. When they dive into the water, they broadcast their position information to help ordinary nodes to calculate their positions. There is also another scheme [51] which consists of four types of nodes that are surface buoys, DETs (Detachable Elevator Transceivers), anchor nodes and ordinary nodes. In this scheme, surface buoys are equipped with GPSs. DET is attached to a surface buoy and it can rise and down to broadcast its position. This scheme increases the localization accuracy and decreases the cost of the system.

Those schemes deal with localization problem; however, in our scheme we deal with key distribution problem. Nevertheless, we are inspired from architecture of the network architecture of the above systems. They use surface buoys for GPS communication; whereas we used them for reducing underwater communication. When it is needed, some heavy communications is handled airborne instead of underwater. In our scheme, similar to [51], there are surface buoys and elevators. Elevators are moving in y coordinate and they are attached to surface buoys with a cable, which provides them a communication capability. There are also ordinary nodes in groups who are communicating with their own elevators. Figure 3.1 shows the architecture of the scheme.

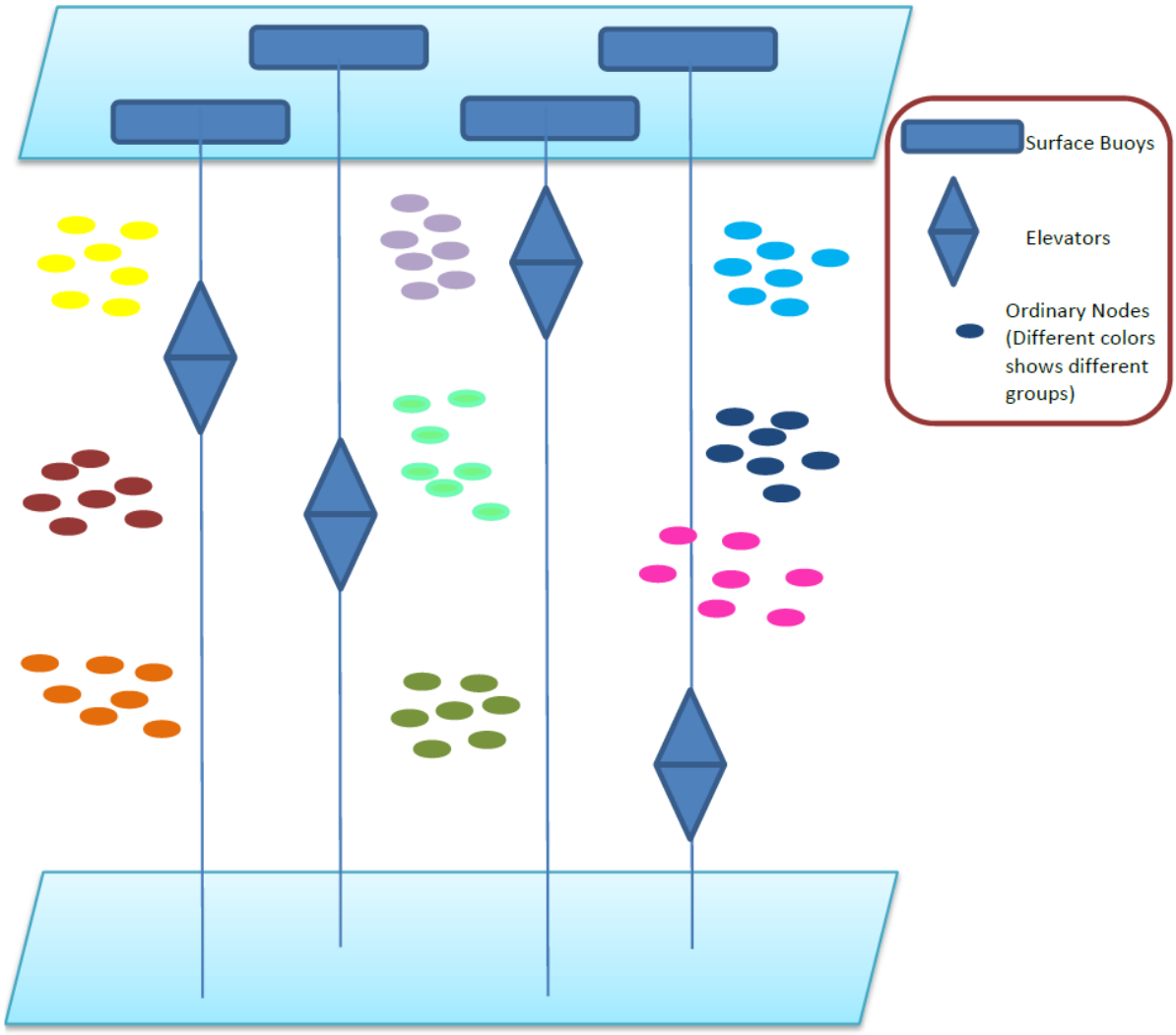


Figure 3.1 Network structure of nomadic mobility based model

In Figure 3.1 there are three types of nodes. Surface buoys are communicating among themselves airborne. Each surface buoy is attached to an elevator which moves up and down in the sea. Each group of node can only communicate with its own elevator. Also each group of nodes can communicate within its group. Thus, it is obvious that there is a hierarchy as can be seen in Figure 3.2. In this figure, there is an example of a hierarchy which has 3 surface buoys and 3 elevators. Each elevator has 3 groups and each group has 15 nodes.

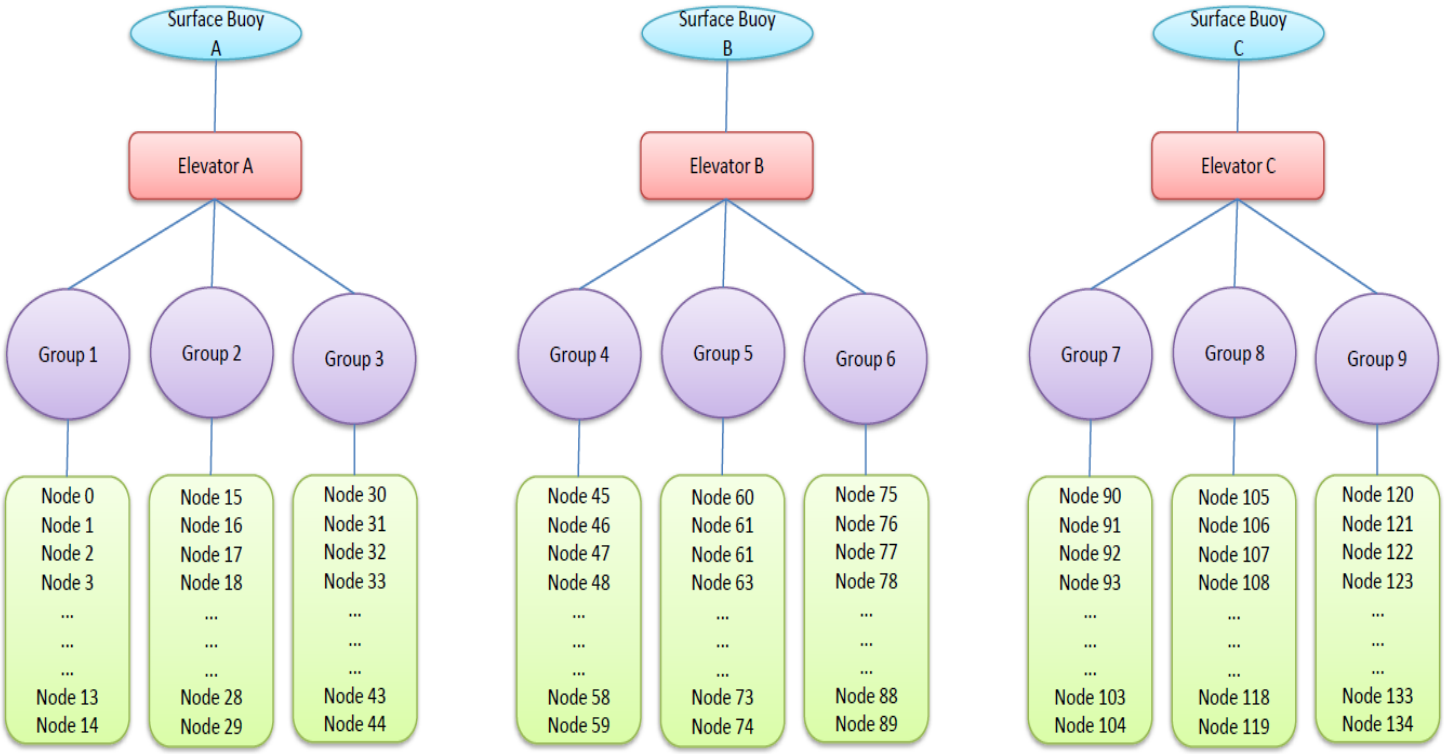


Figure 3.2 Hierarchy of 3 Elevators, 3 Surface Buoys, 9 groups and 135 nodes.

3.2 Communication Patterns in Nomadic Mobility Based Model

In our scheme there are five types of communication patterns. They are: (i) elevator to elevator, (ii) elevator to node, (iii) node to node in same group, (iv) node to node in different groups that belong to same elevator and (v) node to node in different groups that belong to different elevators.

Before giving information about elevator communication, it is important to state the assumptions about elevator and surface buoy relationship in this work. It is assumed that surface buoys are communicating with elevators through a cable and surface buoys have large memory and computational power. In addition it is assumed that they cannot be captured by the adversary. According to these assumptions as surface buoys have large memory, elevator to elevator communication is handled with surface buoys through the air with a pairwise key. Each elevator pair will have different keys, which enhances security. Also, as it is explained above, it is important to reduce the communication overhead for underwater sensor networks. Airborne communication

among surface buoys would increase the performance of the model since airborne communication is less costly.

Also, each node can communicate with elevator by using a pairwise key. Since elevator's memory and computation is assumed to be large, it is not a burden for an elevator to have different keys for each node in its memory. Then each node is loaded with a pairwise key for communication with its elevator.

In addition, reducing communication overhead policy is applied for node to node communication within the same group as well. Blom's scheme is utilized in our scheme, as it is one of the best schemes that has low communication cost [53]. In the hierarchical architecture explained in Section 3.1, the nodes are grouped. Moreover, each group has its own Blom's key space. Thus, if there are p groups for each elevator, then each elevator is loaded with p key spaces.

Symbolically, in Blom's scheme key space is a symmetric matrix, $K = AG$, where G is public matrix and A is private matrix. If p groups are connected to Elevator t, EL_t , then EL_t is loaded with $\{A_0,G_0, A_2,G_2, \ldots, A_{p-1},G_{p-1}\}$. If node h belongs to Group f, then it will be loaded with h th raw of the private matrix A_f. In other words, only nodes in the same group can communicate to each other, as they cannot calculate a common key if they belong to different groups.

Node to node communication in different groups, but in the same elevator is handled via the elevator. If a node from a group wants to communicate with a node from another group that belongs to same elevator, it needs to send a request to its elevator. As elevator can also communicate with the requested node, elevator determines a random pairwise key for those nodes' communication, and sends this key to both of nodes in a secure way. Then the communication between those nodes continues with this key. This protocol is explained symbolically in Figure 3.3. n_a tries to communicate with n_b. Those nodes belong to the same elevator called EL_A. n_a firstly sends its request to EL_A which generates a pairwise key for n_a and n_b. Then, EL_A sends the generated key to both parties. Then they secure messages by encrypting/decrypting with this key.

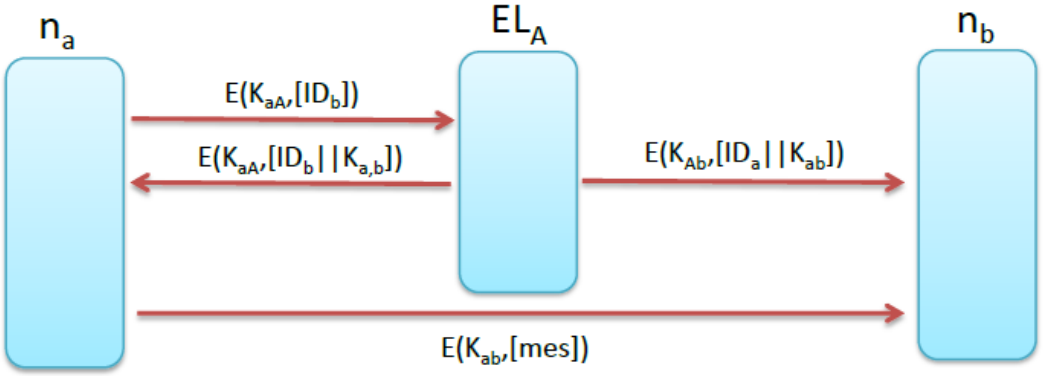


Figure 3.3 Protocol for node to node communication in different groups, but in the same elevator

Node to node communication in different groups and different elevators is established by the communication of the elevators. If a node from a group wants to communicate with a node from another group that belongs to a different elevator, then it sends a request to its own elevator. This elevator communicates with corresponding elevator which has the requested node. Then these elevators agree on a key for the communication of those nodes. Then, they send this key to their corresponding nodes in a secure way. For future communications those nodes use this established key. This protocol is explained symbolically in Figure 3.4. Also all these communication types are summarized in Figure 3.5.

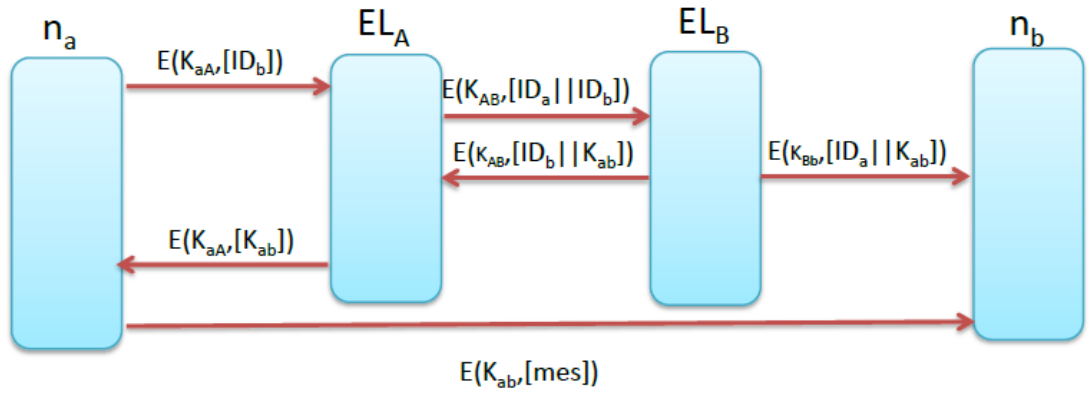


Figure 3.4 Protocol for node to node communication in different groups and different elevators

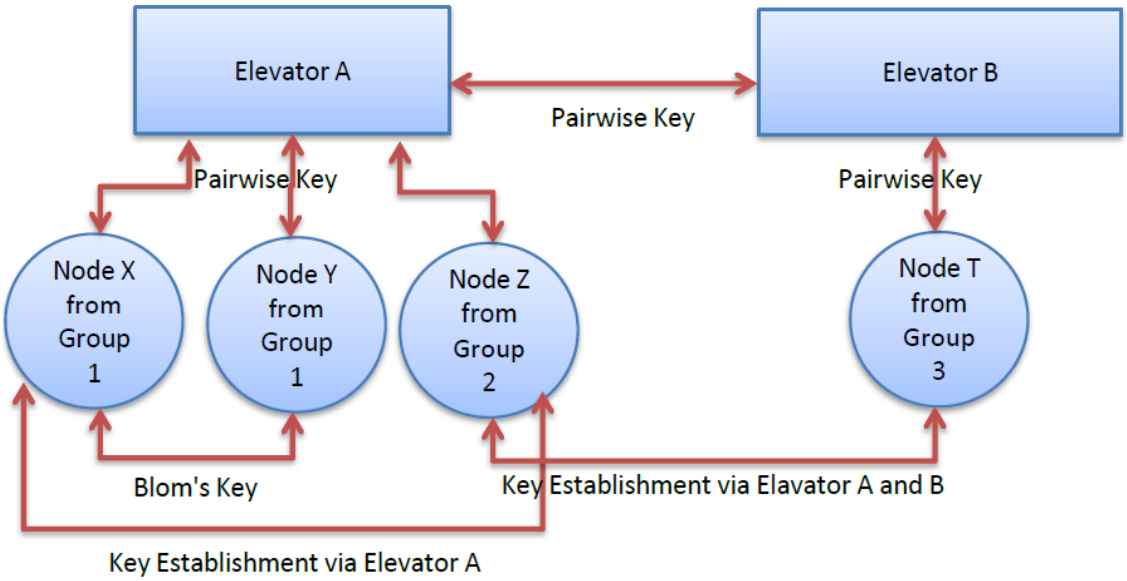


Figure 3.5 Communication patterns in our hierarchical architecture and corresponding key establishment mechanisms

3.3 Nomadic Mobility Model

Nodes in underwater cannot be static because of the external effects. In underwater there are several factors such as current and living creatures that drift nodes. For this reason, the scheme should consider the mobility of the nodes. The most powerful expected effect is the wave. As we assume that our scheme is suitable for sea shore not for deep sea, nodes will be affected from the same force of wave. It means that mobility of all nodes have the same direction. Then there is group mobility. In addition each node can also be affected from small other factors like fishes.

The most similar model with these properties is nomadic community model. As it is explained in Section 2.5, nodes are drifted together to a place and then in this new place, each node makes small movements independently in a random way. In our scheme, there are groups and those groups move with a stream to a direction and each node moves slightly from its new place.

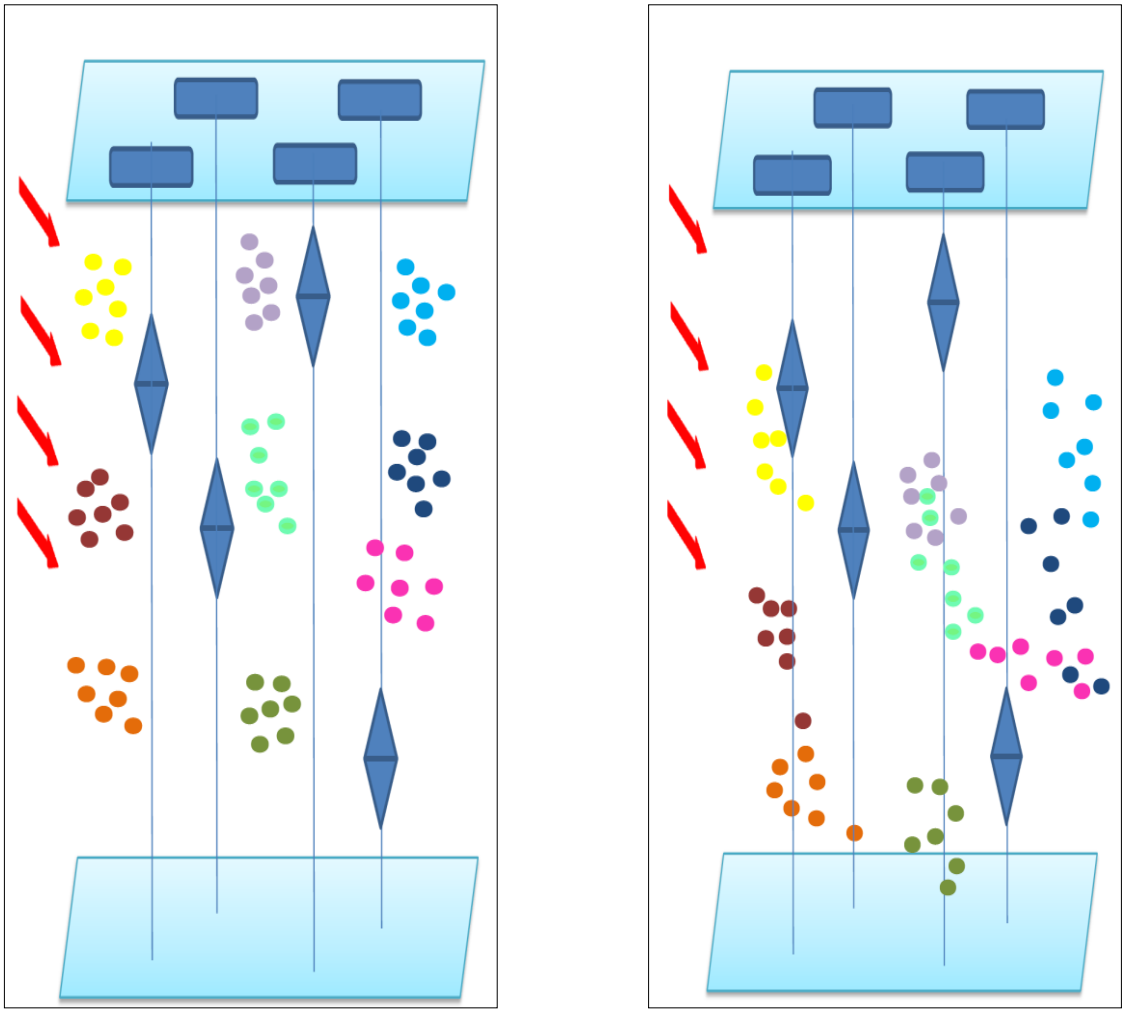


Figure 3.6 Nomadic mobility of nodes

The left figure in Figure 3.4, shows the initial position of nodes. Nodes are affected by the stream that is shown as red arrows. All nodes move in the direction of that arrow for a time period. After that, they reach to a new place, and then each node changes its place slightly. After a while this movement results in mixture of different groups of nodes. Also some nodes fall behind and break away from its group. Here, our scheme fixes this disengagement of nodes. Elevators have vital mission to prevent break of nodes from other nodes. While the elevators are diving and rising, they sense the groups of nodes in its range. If the number of nodes that belong to a group is very low, then it means that these nodes have been broken away from its group. Then these nodes should be included to the nearest group. This is handled by elevators. That entire scenario is explained in detail in the following section.

3.4 Key Establishment Phases

Key establishment can be examined in three phases: before deployment, after deployment and after movement phases. These phases are explained in details in following subsections. Also Table 1 contains the symbols that are used in this section.

nd_i	Node with ID i
SB_a	Surface buoy with ID a
EL_a	Elevator with ID a
$SBEL_a$	Surface buoy & elevator with ID a
gr_c	Group with ID c
A_c	Private matrix A of group gr_c
G_c	Public matrix G of group gr_c
M	Total number of surface buoy & elevator units
P	Total number of groups
H	Total number of nodes
C	Number of nodes per surface buoy & elevator units
T	Number of nodes per group
K_{xy}	Key between entity x and y where both can be a surface buoy and elevator unit or a node
$E\ (K, [mes])$	Encryption of a message mes with a key K
rp	Redundant parameter
WG	Set of waiting groups to be added to the nearest group
cdr	Clustering determination ratio
$ReqMes$	Request Message

Table 1 Symbols used in this section

3.4.1 Before Deployment

Initially, all surface buoys are loaded with pairwise keys for secure communication between other surface buoys. As there is a cable which provides instant communication between a surface buoy and its corresponding elevator, we can see the surface buoy and the elevator as the same operational unit. For this reason, we use surface buoy & elevator combined unit for the following operations. Each surface buoy & elevator unit is loaded with pairwise keys that provide secure communication between the elevator and its nodes. Each surface buoy & elevator unit calculates Blom's matrices for each group of node which belongs to this elevator. Public and private matrices (A and G matrices) of each group are loaded to the memory of owing surface buoy & elevator unit.

Symbolically surface buoy SB_a and elevator EL_a are combined as the same operational surface buoy & elevator unit as $SBEL_a$. Each $SBEL_a$ where $a = 1 \dots M$ and M is the total number of surface buoy & elevator units, is loaded with A_c and G_c matrices of each group gr_c where $c = 1 \dots C$ and C is the number of groups that belong to a $SBEL$.

Each node is firstly loaded with a unique ID. Then it is loaded with a pairwise key for secure communication with its elevator. Also it is loaded with private parameters which is a row of its group's Blom Private Matrix (A). Suppose that node nd_i belongs to a group gr_c which belongs to a surface buoy & elevator $SBEL_a$. Then this node will be loaded with ID i, ID a and a row of private matrix A_c .

Suppose that M is the number of $SBEL$s and C is the number of groups per $SBEL$. Also each group contains T number of ordinary nodes. Then each $SBEL_a$, $a = 1 \dots M$ have $M - 1$ number of different pairwise keys to communicate with each surface buoy & elevator unit. Each $SBEL_a$ also has $C.T$ number of pairwise keys, for node communications. Also each of $SBEL_a$ has C number of public G and private A matrices. The size of public matrix is $Tx\lambda$ and private matrix is $\lambda x T$ where λ is security threshold. If we want our scheme to be resilient to attacks, then this parameter should be large. Also, according to our scheme, some nodes will be added to the groups during the operation. Then node per group changes in time. In order to compensate this change, we

need to have some redundant private and public rows and columns. When a new node is added to the group, a row of private matrix is loaded to this new node. Number of these redundant rows is a parameter which is rp. Then public matrix is $(T + rp)x\ \lambda$ of size and private matrix is $\lambda\ x(T + rp)$ of size. Also each node nd_i which belongs to gr_c and $SBEL_a$, have just one pairwise key, K_{ia} , for communication with $SBEL_a$ and a row of the private key of $A_c$which has λ number of elements.

3.4.2 After Deployment

In our model we use Blom's scheme. We assume that nodes that belong to the same group are deployed together. Also groups belong to an elevator are deployed near to its elevator. Elevator is also diving and rising continually. We assume that nodes are deployed according to Gaussian distribution. After deployment each node tries to find its neighbors by broadcasting its ID. Suppose nd_i which belongs to g_c in $SBEL_a$ tries to find its neighbors. If its neighbor nd_j belongs to the same group g_c, then nd_i calculates their common key K_{ij} by multiplying its private parameters which is row of A_c and the column of public matrix G_c. Similarly, nd_j calculates their common key K_{ji} where $K_{ij} = K_{ji}$. After that, they talk securely with this calculated common key. If the neighbor node nd_j belongs to another group g_d which belongs to same surface buoy & elevator unit $SBEL_a$, then they should establish a key via $SBEL_a$. $SBEL_a$ determines a random pairwise key K_{ij} for those nodes and it sends this key to nd_i and nd_j by using keys K_{ai} and K_{aj} in a secure way. After that these nodes use this key for their communication. If the neighbor node nd_j belongs to another group $g_d$which is owned by a different surface buoy and elevator unit $SBEL_b$, then these nodes can provide their key with the help of $SBEL_a$ and $SBEL_b$. $SBEL_a$ and $SBEL_b$ agree on a key K_{ij} which is used for those nodes communication. This process is provided by the communication of surface buoys airborne. This established key K_{ij} is sent by $SBEL_a$ and $SBEL_b$ to nd_i and nd_j. All these operations are explained in pseudo code at Figure 3.7.

Suppose that nd_i belongs to g_c in $SBEL_a$ and its neighbor nd_j belongs to g_d in $SBEL_b$.
for all $nd_i, i \in H$

Send ReqMes

if(nd_j, $j \in H$, receives ReqMes)

if($g_c == g_d$)

nd_i calculates K_{ij} and nd_j calculates K_{ji}

end

else if($SBEL_a == SBEL_b$)

$SBEL_a$ generates K_{ij} sends it to nd_i and nd_j by using K_{ai} and K_{aj}

end

else

$SBEL_b$ generates K_{ij} and sends it to $SBEL_a$ and nd_j by using K_{ba} and K_{bj}

$SBEL_a$ sends K_{ij} and to nd_i by using K_{ai}

end

end

end

Figure 3.7 Pseudo code of after deployment phase

3.4.3 Operational Phase:

After key establishment phase is completed, communication between nodes starts. Nodes are drifted because of waves in the sea. We modeled this mobility model according to nomadic group mobility model [29]. In this model, nodes go with a random speed and direction for a while. Then each node move slightly with random speed to a random direction. While nodes are moving, their neighbors are changing. For this reason, elevators connect new neighbors and fix up the groups. While elevator is rising and diving, it constantly sense around to understand how many groups and nodes are in its range. It tries to sense if any node is drifted away from its group. Elevator realizes this by determining a clustering determination ratio. If the number of nodes that belong to a group is smaller than this ratio, it means that these nodes have been drifted away from its own group and should be included to a nearer group. For this aim, the nearest group whose number of nodes in elevator's range is larger than clustering

determination ratio, is found. Then the nodes which are drifted away from its group are added to that group. Four different cases may occur here:

Suppose that $SBEL_s$ realizes x groups in its range. y of x groups have more number of nodes than the clustering determination ratio cdr. Then nodes in $x - y$ groups in range of $SBEL_s$ are waiting to be added to another group. This set of groups who are waiting to be added to another group is expressed as WG. Also, nd_i is a node from gr_t which belongs to $SBEL_a$ and it is in range of $SBEL_s$. The nearest group that this node is planned to be added is gr_n which belongs to $SBEL_b$ and it is in the range of $SBEL_s$.

- If additive node nd_i and the group that it will be added gr_n , belong to the sensing surface buoy & elevator unit $SBEL_s$, then $SBEL_s$ sends a new private parameter raw from A_n which is the new group's private matrix (one of the redundant rows of A_n matrix from this $SBEL_s$'s Blom key space) and new group ID to additive node nd_i.
- If additive node nd_i belongs to the sensing surface buoy & elevator unit $SBEL_s$ but the group gr_n does not belong to $SBEL_s$, then $SBEL_s$ communicates with gr_n's surface buoy & elevator unit $SBEL_b$ and gets a row of private matrix A_n airborne. Then $SBEL_s$ sends this row and new group ID to additive node nd_i.
- If group gr_n belongs to the sensing surface buoy & elevator unit $SBEL_s$ but node nd_i does not belong to $SBEL_s$, then $SBEL_s$ communicates with the owing surface buoy & elevator unit $SBEL_a$ airborne and gets a secure communication key K_{is} to communicate with this node and sends a row from A_n and new group ID to additive node nd_i.
- If both the node nd_i and the group gr_n does not belong to the sensing surface buoy & elevator $SBEL_s$, then $SBEL_s$ firstly communicates with the owing surface buoy & elevator unit $SBEL_b$ of the group gr_n airborne and gets a row from A_n for a new node. Then surface buoy & elevator unit $SBEL_s$ communicates with $SBEL_a$ which is the owing surface buoy & elevator unit of the additive node nd_i. $SBEL_s$ gets a secure communication key K_{is} to communicate with this node and sends the row from A_n and new group ID to additive node nd_i.

All of these operations are explained in Figure 3.8. After all these operations, node nd_i erases its old private parameters and establishes new links with its new neighbors. This operation prevents breakaways and provides all nodes be connected to the network. Also, as most of the communications are handled airborne, it does not lead to much communication overhead.

for all nd_i which is in the range of $SBEL_s$ and belongs to gr_c in WG and gr_c belongs to $SBEL_a$
    Find nearest group gr_n and it belongs to $SBEL_b$
    if($SBEL_s == SBEL_a \;\&\&\; SBEL_s == SBEL_b$)
        $SBEL_s$ sends a row from A_n and new ID to nd_i
    end
    else if ($SBEL_s == SBEL_a \;\&\&\; SBEL_s !== SBEL_b$)
        $SBEL_s$ sends a ReqMes for a row from A_n to $SBEL_b$
        $SBEL_b$ sends a row from A_n to $SBEL_s$
        $SBEL_s$ sends a row from A_n and new ID to nd_i
    end
    else if ($SBEL_s !== SBEL_a \;\&\&\; SBEL_s == SBEL_b$)
        $SBEL_s$ sends a ReqMes for a key K_{is} to $SBEL_a$
        $SBEL_s$ sends K_{is} to $SBEL_s$
        $SBEL_s$ sends a row from A_n and new ID to nd_i
    end
    else
        $SBEL_s$ sends a ReqMes for a row from A_n to $SBEL_b$
        $SBEL_s$ sends a ReqMes for a key K_{is} to $SBEL_a$
        $SBEL_b$ sends a row from A_n to $SBEL_s$
        $SBEL_a$ sends K_{is} to $SBEL_s$
        $SBEL_s$ sends a row from A_n and new ID to nd_i
    end
end

Figure 3.8 Pseudo code of operational phase

3.5 Implementation Details

Simulation of this model is implemented on Visual Studio 2010 environment and used C# for coding. In our simulation there are 960 nodes that are deployed as two

layers by using Gaussian distribution model. There are 32 groups that each group has 30 nodes. Simulation area is $200m * 200m * 200m$. There are four elevators and four surface buoys. Sensor range is 50 meters [53] and each sensor's speed is maximum 3.6 m/min. Elevator's speed is constant with amount of 5 m/min. Packet energy consumption values are calculated in [54]. They have measured average packet delay and average energy consumption per packet for different type of MAC layers. We chose RMAC model as it is much more energy efficient than the others. RMAC's average energy consumption per packet is 70 milijoule. Besides, there is also energy consumption for encryption and decryption operations. AES encryption/decryption is used for symmetric key cryptography. Underwater network's nodes are built around a CPU unit based on ATmega128 microcontroller [55] and it consumes 1.62 µjoule/byte for encryption and 2.49 µjoule/byte for decryption [56]. According to those values we have performed our simulation and get the following results.

3.6 Performance Evaluation

We perform simulations of our proposed scheme to evaluate the results according to the metrics. Those metrics are secure connectivity, resiliency against node capture attacks and battery consumption. Secure connectivity is the probability of sharing common key between any two neighbor nodes. Also, resiliency is analyzed in two metrics called additionally compromised links ratio and total compromised links ratio. Battery consumption is the energy cost of key distribution operations for each node. Those metrics are explained in details in following subsections. Also performance results are illustrated in graphs in following subsections.

3.6.1 Secure Connectivity

Secure connectivity is an important metric to show the quality of key distribution schemes. It is the probability of any two neighboring nodes sharing a common key. Figure 3.9 shows the secure connectivity of our scheme based on nomadic mobility model.

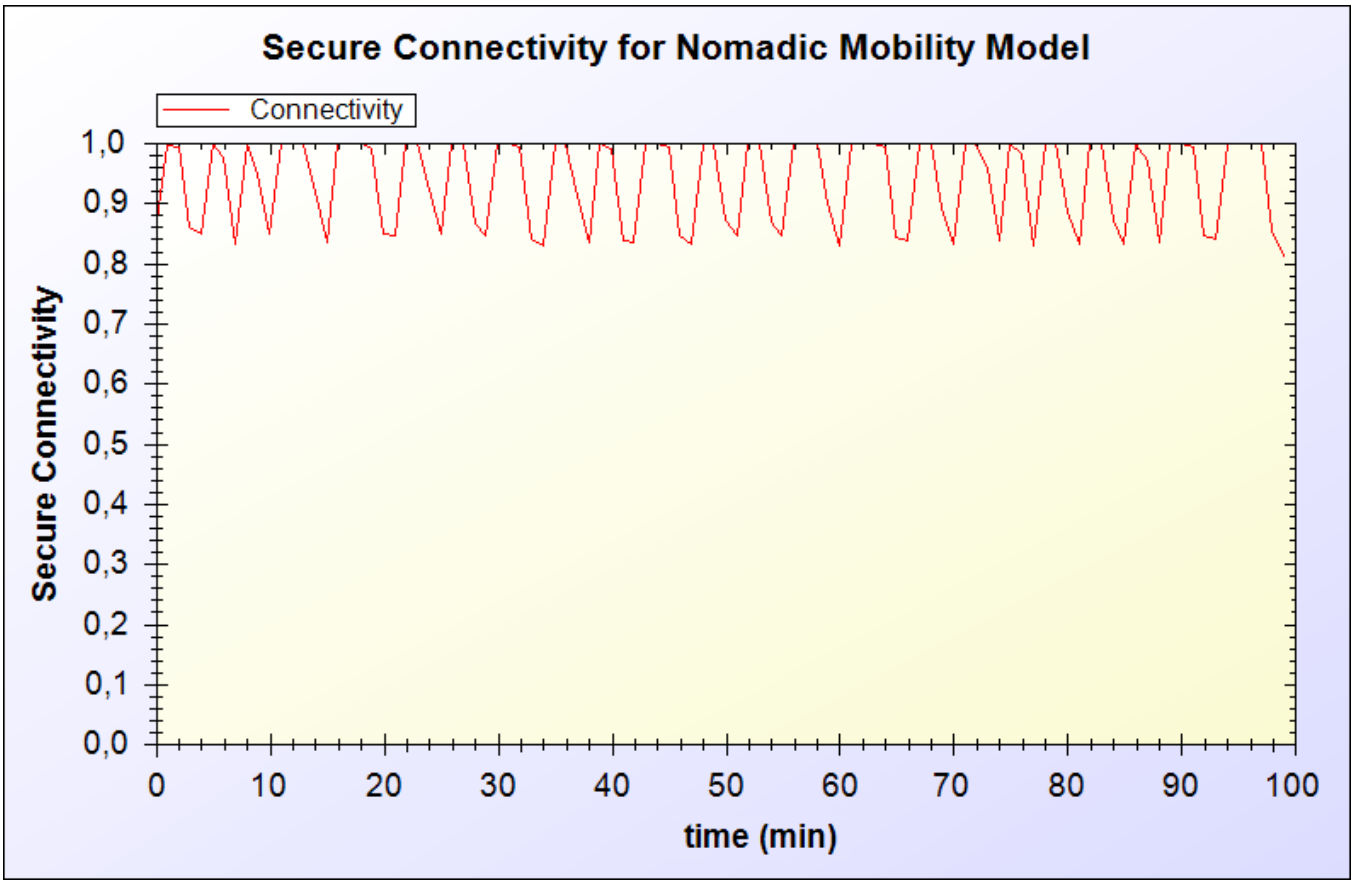


Figure 3.9 Secure connectivity for nomadic mobility based model

Nodes are mobile and nodes in the same group shares key in this scheme. Because of this mobility, some of the nodes are drifted away and for a while these nodes are surrounded with nodes which do not belong to the same group. Then they will not be connected to the graph which results in decreasing the connectivity. However as our model includes elevators which connect those drifted nodes to nearing groups, connectivity refreshes itself and become 1.0. This model results in zigzags in secure connectivity graph and this model heals itself in terms of connectivity when it falls.

3.6.2 Resiliency against Node Capture Attacks

An attacker can capture nodes in an underwater network. As nodes generally are not tamper proof, attacker can reach the keys of the nodes. After attacker learns the keys of the captured node, he can use this node as an agent to learn about the communications by putting the captured node the network again. It can decrypt messages that are sent to or sent by this captured node. In addition, if any of the keys of

this captured node is used between non-captured nodes, then attacker captures the link between these non-captured nodes. Additionally compromised link ratio (additionally compromised links / all links) is a measure that shows how many extra links are reached by the attacker after some are captured. In other words, communication links of the captured nodes are not included. In contrast, total compromised link ratio (total compromised links / all links) includes all links that are captured by the attacker. In a sense, total compromised link consists of not only all the links of captured nodes but also extra links that uses a captured key between non-captured nodes.

In our scheme, Blom's scheme which has λ-security, is used. In Blom's scheme λ is the threshold. When the number of captured nodes exceeds λ, then all keys in the group are revealed. Thus, similarly in our scheme resiliency ratios depend on the value of λ. If λ is larger, the memory size needed for the matrices became larger and since matrices became larger, operations on matrices became larger which results in more energy consumption. In our scheme, group size became larger after a while as drifted nodes are added to nearest group. For that reason, if λ is determined as total of the initial node number per group and redundant parameter which is for prospective additive nodes, then this scheme has perfect resiliency since captured nodes cannot exceed λ in any time. In other words, attacker cannot reach any additional link with the help of captured nodes. However, if λ is larger, nodes consume too much memory and energy for computations. For that reason λ is determined as 10. Number of nodes per group at initial deployment is 30. Also the power of the attacker is determined as 2, 3 and 4 node captures per each minute. Resiliency graphs are illustrated in Figure 3.8 and 3.9.

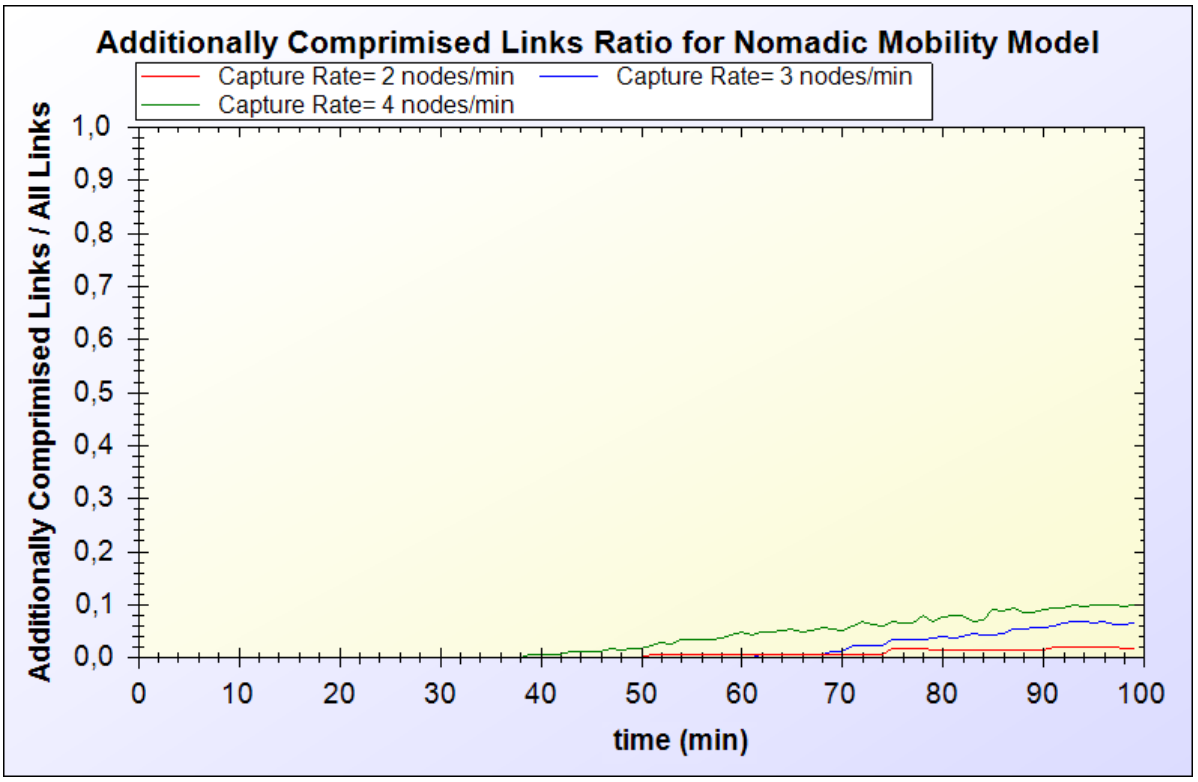


Figure 3.10 Additionally compromised links ratio for nomadic mobility based model

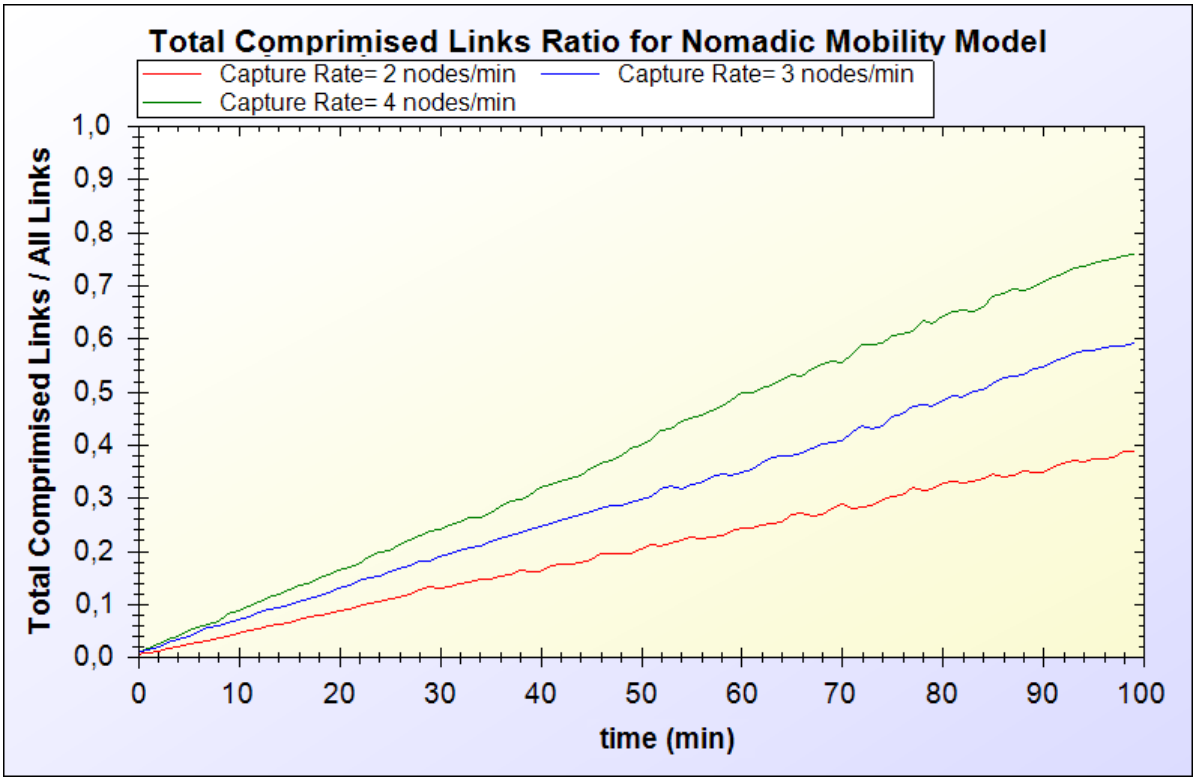


Figure 3.11 Total Compromised links ratio for nomadic mobility based model

As it can be seen from Figure 3.12, at the beginning of the simulation, for a long time there is perfect resiliency since number of captured nodes from each group does not exceed λ. It means that no additional link can be reached by the attacker. However after a while, in some groups number of captured nodes exceeds λ security parameter which means that those group's links are all revealed. Despite some groups are revealed, additional compromise link ratio is still in reasonable amounts, since there is only small number of groups in which captured number of nodes exceeds λ. When node captures per minute increases, additionally compromised links ratio increases as it is expected. For the capture rate of 4 nodes per minute we have largest additional link ratio. Even for this one ratio does not exceed 0.1 which is about perfect resiliency. In Figure 3.11 total compromised links ratio for nomadic mobility is illustrated. At the end of the simulation 200, 300 and 400 of 600 nodes are captured respectively for capture rates of 2, 3 and 4. At the end of the simulation total compromise ratio is 0.4, 0.6 and 0.75 for capture rates 2, 3 and 4 respectively. Also, in this graph it is obvious that total compromised links increases when capture rate increases.

3.6.3 Average Energy Consumption

Energy consumption is a significant issue since wireless sensor nodes are primitive equipments that have small battery power. In our simulation, we measure average battery consumption per node. Communication between nodes and elevator is calculated. Packets are encrypted and decrypted via AES which has 1.62 μjoule/byte energy consumption for encryption and 2.49 μjoule/byte energy consumption for decryption. Also each packet (64 bytes) transmission consumes 70 milijoules. According to those values, Figure 3.10 shows the average energy consumption per node. Each fix up operation of our scheme, causes energy consumption. Since the system makes fix up operation periodically, there is a linear increase in the graph.

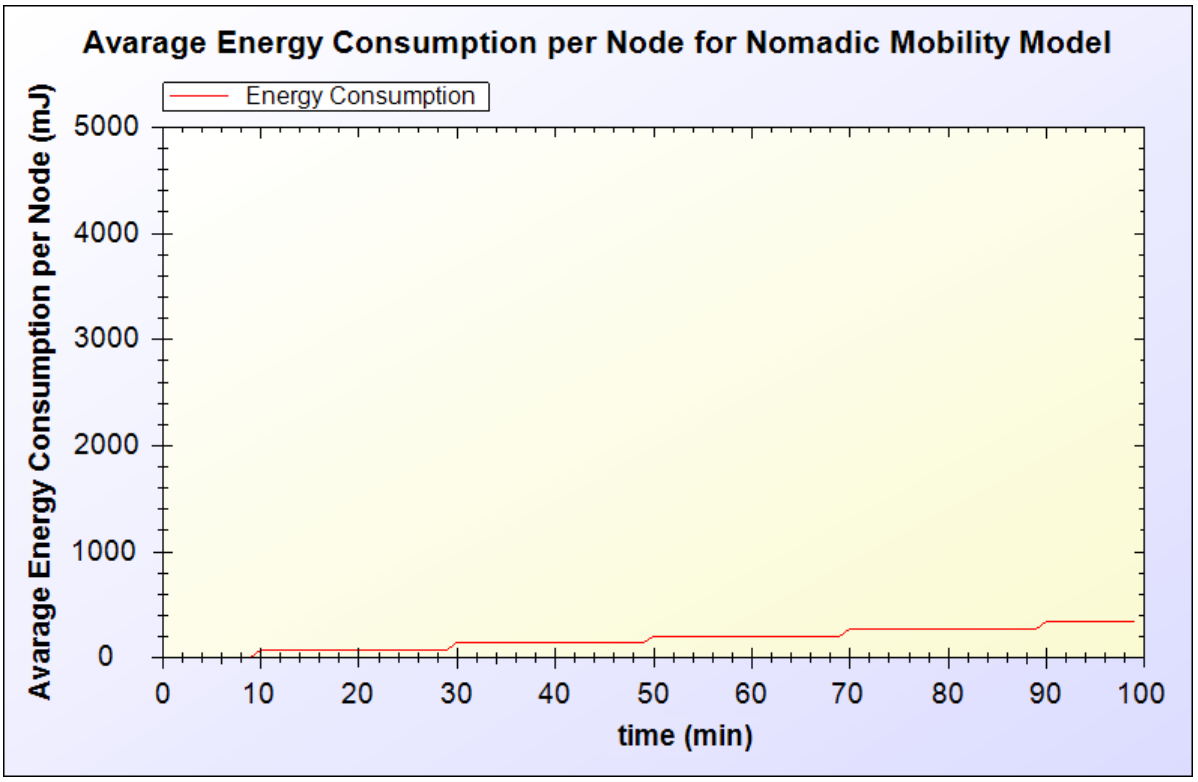


Figure 3.12 Average energy consumption per node for nomadic mobility based model

3.6.4 Memory Requirements

Blom's scheme is utilized in our model. For this reason memory needs depend on Blom's scheme's requirements. This scheme's details are explained Section 2.4. Initially, each node is loaded with its own ID and the ID of the elevator that it belongs to. In addition, each node is loaded with private shares which are elements of a row of a private matrix A. This row has $\lambda + 1$ elements, where λ is the security threshold. Also each node needs to store two parameters s and q, where s is the seed of the Vandermonde matrix and q is the prime number. These parameters are used to generate a column of a Vandermonde matrix.

To sum up, memory requirements are ID of the node, ID of the elevator, a row of private matrix, s and q. The length of each of these values is the symmetric key length. Thus we assume that 128-bit symmetric keys are to be generated, then total memory requirement becomes $(\lambda + 5)$ x 128 bits. In our simulations, $\lambda = 10$, our memory requirement per node is 240 bytes.

Chapter 4

A Key Distribution Scheme for Underwater Sensor Networks with Meandering Current Mobility Model

4.1 Network Architecture of Meandering Mobility Based Model

This scheme is proposed as a large-scale oceanographic model. In contrast to nomadic mobility based model, meandering mobility based model is designed as boundless and it is for large ocean environments that spans several kilometers in much longer time. Also as meandering mobility model does not consider vertical movements, this scheme is designed as two dimensional model.

Hierarchical structure is used as similar to our nomadic mobility model; however, since the model is two dimensional, we do not use elevator that moves towards the vertical axis. This time, surface buoys are connected to underwater devices which are fixed to the ground of the ocean. Also surface buoys are communicating through the air and each surface buoy communicates with its underwater device via a cable. Ordinary nodes are grouped and each group can only communicate with its own underwater device. Then each underwater device have several number of groups. Figure 4.1 shows the architecture of the scheme.

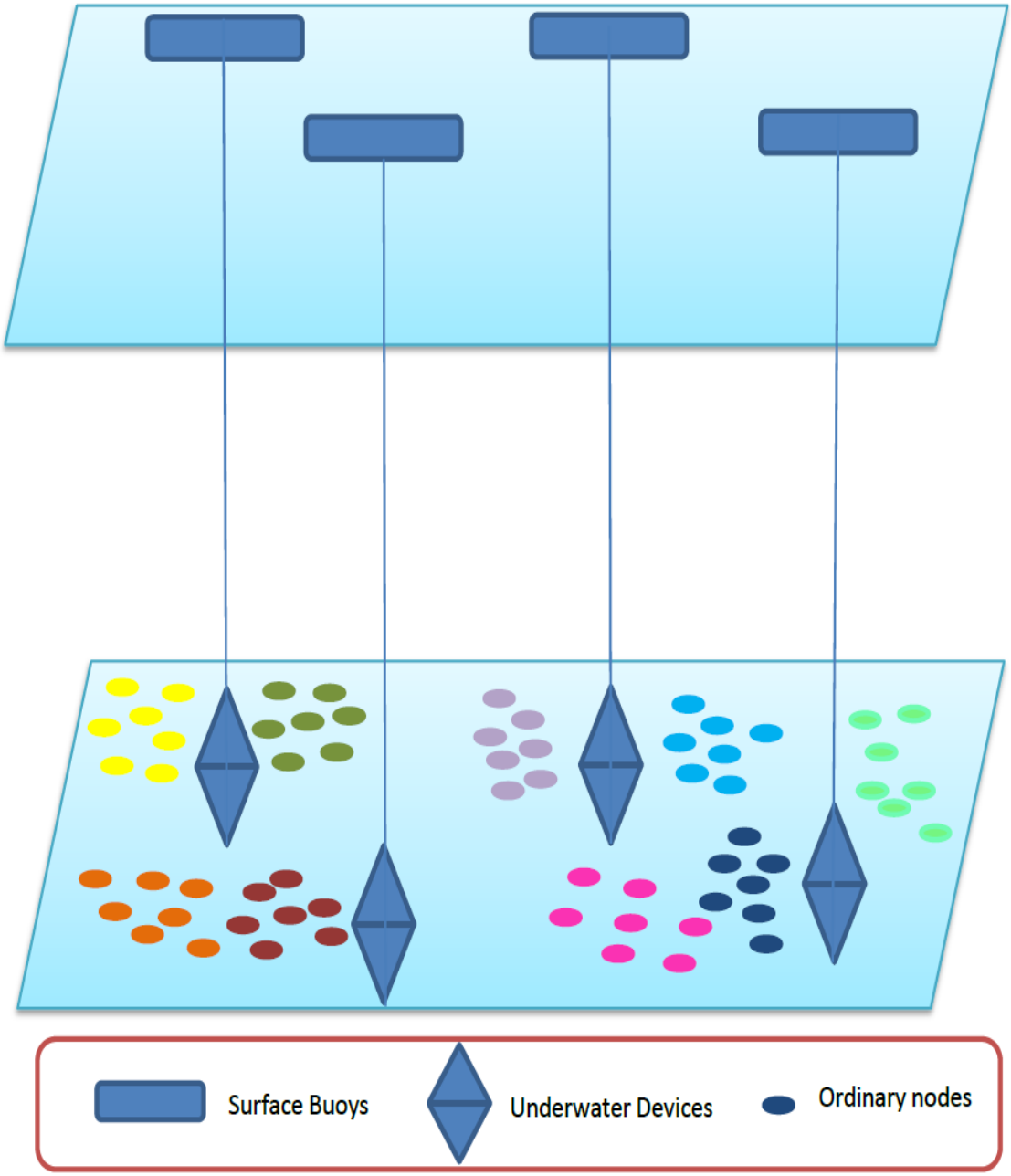


Figure 4.1 Network structure of meandering mobility based model

4.2 Communication Patterns in Meandering Mobility Based Model

Network structure of the scheme based on meandering mobility has similar components with the model based on nomadic mobility, communication patterns are also similar. The patterns are as follows: (i) underwater device to underwater device, (ii) underwater device to node, (iii) node to node in same group, (iv) node to node in

different groups that belong to same underwater device and (v) node to node in different groups that belong to different underwater devices.

Underwater device to underwater device communication is handled with surface buoys through the air with a pairwise key. Also, underwater device to node communication is constructed by the help of a pairwise key. As Blom's scheme is used, node to node communication in same group is established via Blom's key. Node to node communication in different groups that belong to same underwater device is handled by the help of their underwater device. This underwater device communicates with both of the nodes and determines a key for their communication. Node to node communication in different groups that belong to different underwater devices is established via the communication of their underwater devices. These underwater devices agree on a key and sent this key to the nodes. Then this key is used for these nodes' communication.

4.3 Details of Meandering Mobility Model

Nomadic mobility model is kind of an hypothetical model despite the fact that it seems reasonable. Meandering mobility model is more realistic since it captures the dynamics of the water. The meandering current mobility model [33] is a model which considers the movements of ocean. In this work, we proposed a key distribution model based on meandering current mobility model, in order to make our model more realistic. The proposed scheme is similar to the one proposed for nomadic mobility model, but the most important difference is meandering mobility model captures dynamics of the ocean. In this model nodes are spanning several kilometers in longer time. However this model is two dimensional since ocean's vertical movements are negligible with respect to horizontal ones.

In meandering mobility model two dimensional flow is described by a stream function Ψ. By the help of this function, displacement of nodes in x and y coordinate can be found. This stream function in [33] is given as follows where the symbols are given in Table 2:

$$\Psi(x,y,t) = -\tanh\left[\frac{\mathrm{y}-\mathrm{B(t)}\sin(\mathrm{k(x}-\mathrm{ct))}}{\sqrt{1+k^2B^2(t)cos^2(k(x-ct))}}\right] \text{ where } B(t) = A + \epsilon\cos(wt)$$

k	Number of meanders in unit length
c	Phase speed with which they shift downstream
B	Width of the meanders
A	Average meander width
ϵ	Amplitude of the modulation
w	Frequency

Table 2 Stream Function's variables

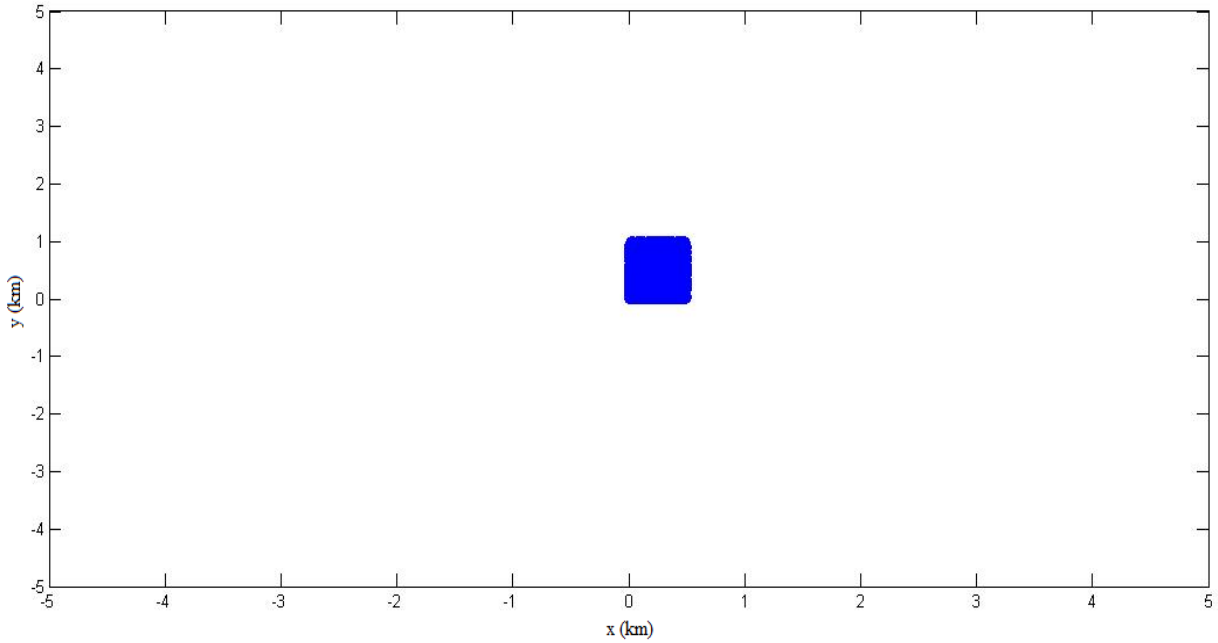
This stream function describes a current, due to meandering between recirculating vortices. In our simulations these variables are same as in [33]: $A = 1.2$, $c = 0.12$, $k = 2\,\pi/7.5$, $w = 0.4$ and $\epsilon = 0.3$. One dimensional unit of space is a kilometer whereas unit of time is 0,03 days. Each sensor's displacement in x and y coordinate is found as:

$$\mathrm{xdisplacement} = -\,\partial\mathrm{y}\,\Psi(\mathrm{x},\mathrm{y},\mathrm{t}) * \partial\mathrm{t}\,\Psi(\mathrm{x},\mathrm{y},\mathrm{t})$$

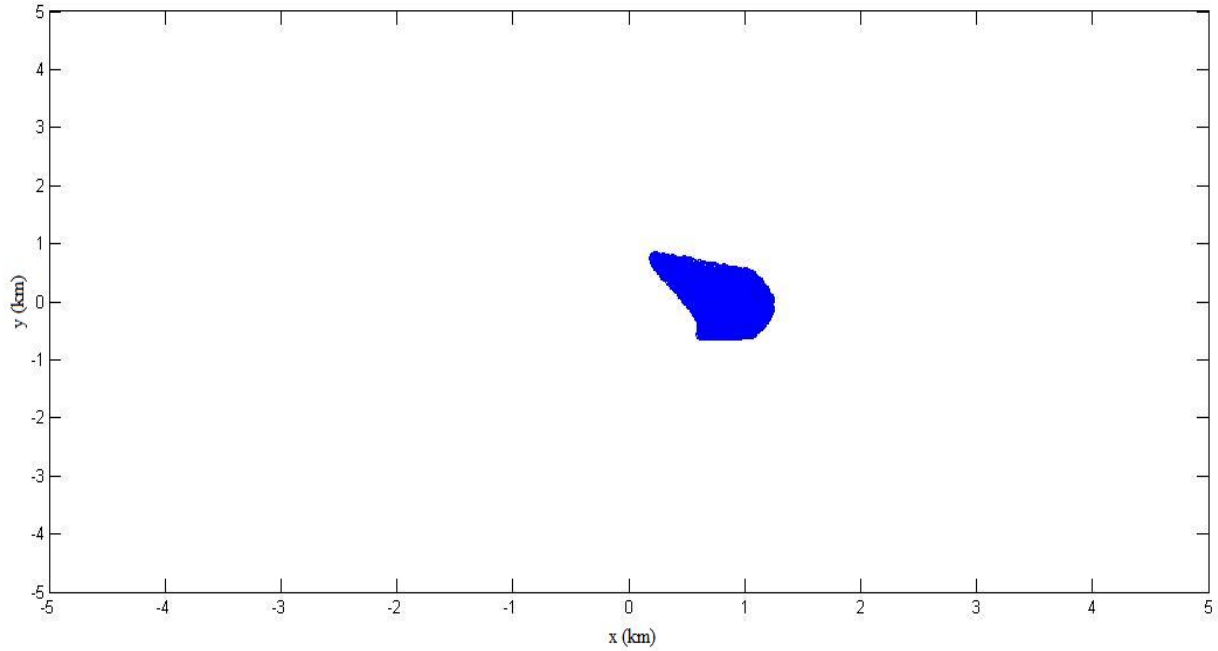
$$\mathrm{ydisplacement} = \partial\mathrm{x}\,\Psi(\mathrm{x},\mathrm{y},\mathrm{t}) * \partial\mathrm{t}\,\Psi(\mathrm{x},\mathrm{y},\mathrm{t})$$

According to these equations we have simulated the mobility model for 3 days (time = 100*0.03 days) for 6000 nodes deployed in 0.5 km x 1 km. Screenshots for each 10 time unit is shown in Figure 4.2.

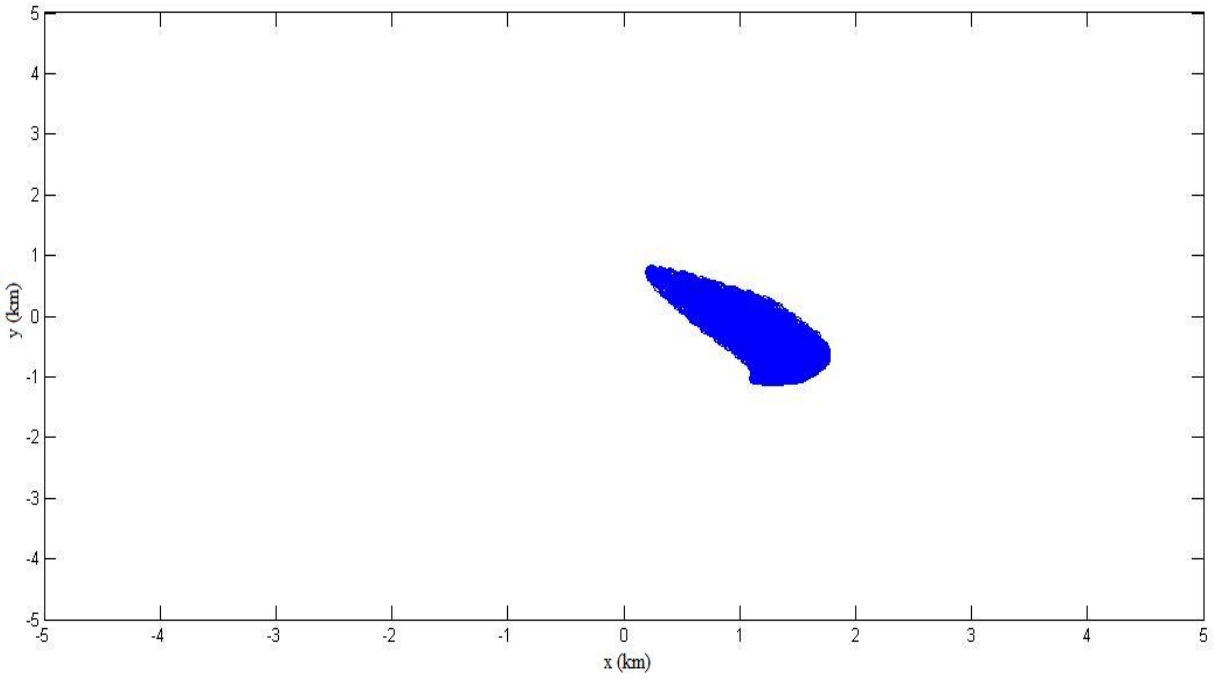
Time = 0 unit



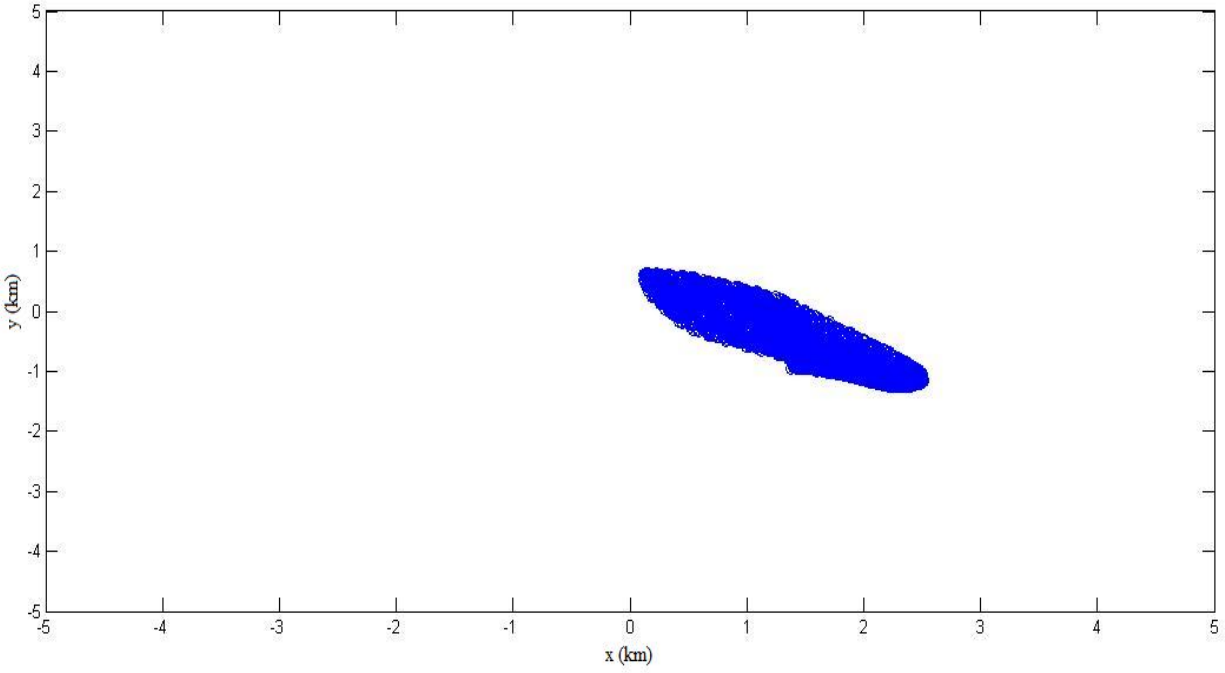
Time = 10 unit



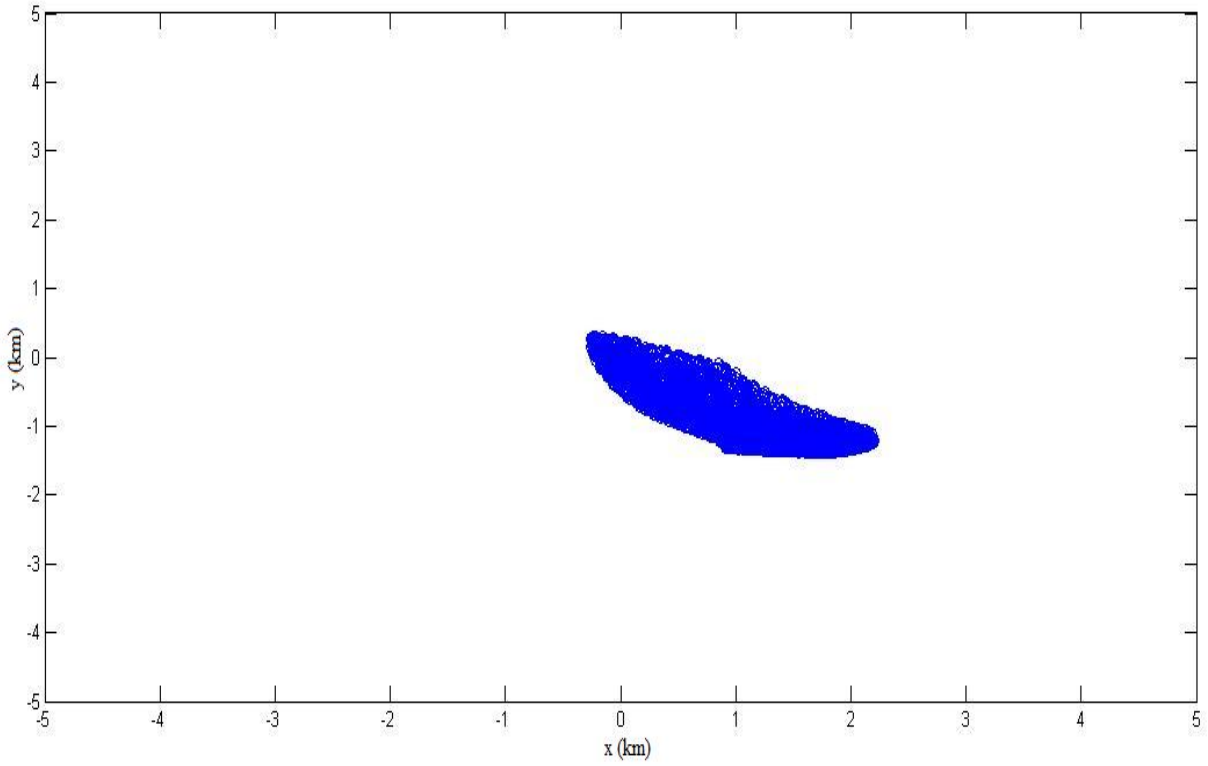
Time = 20 unit



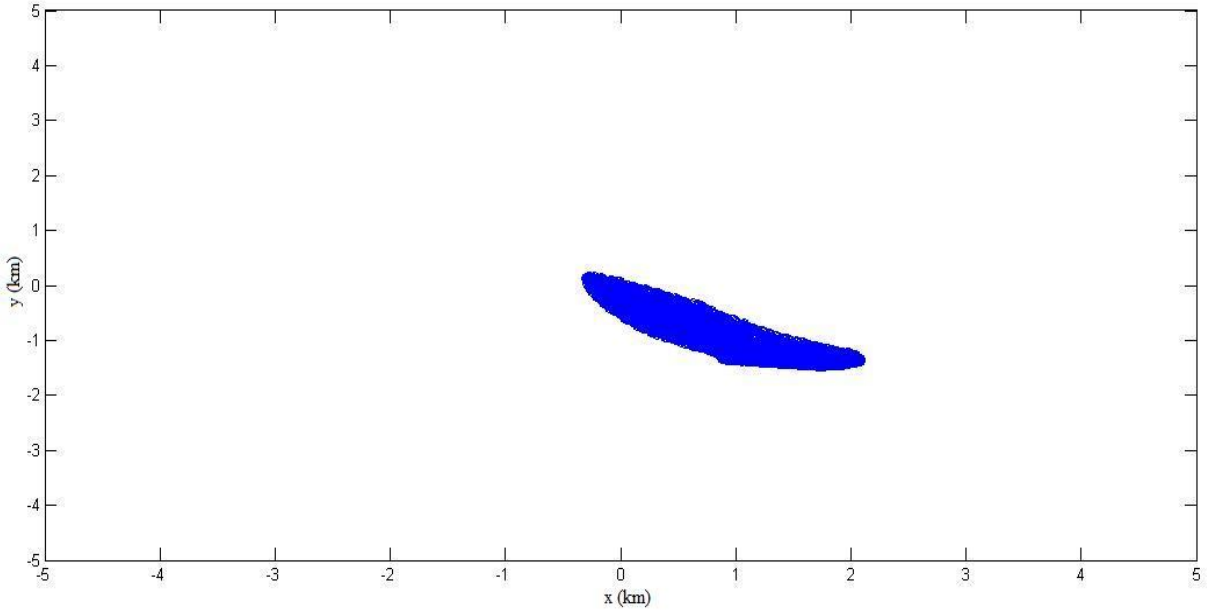
Time = 30 unit



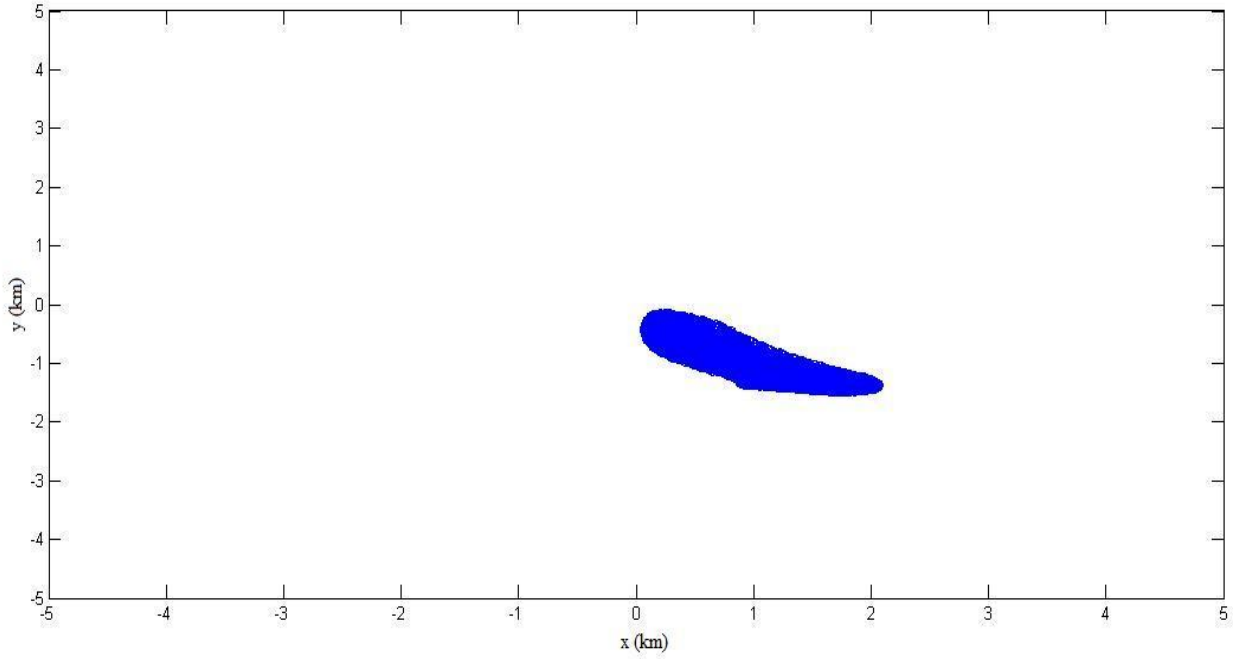
Time = 40 unit



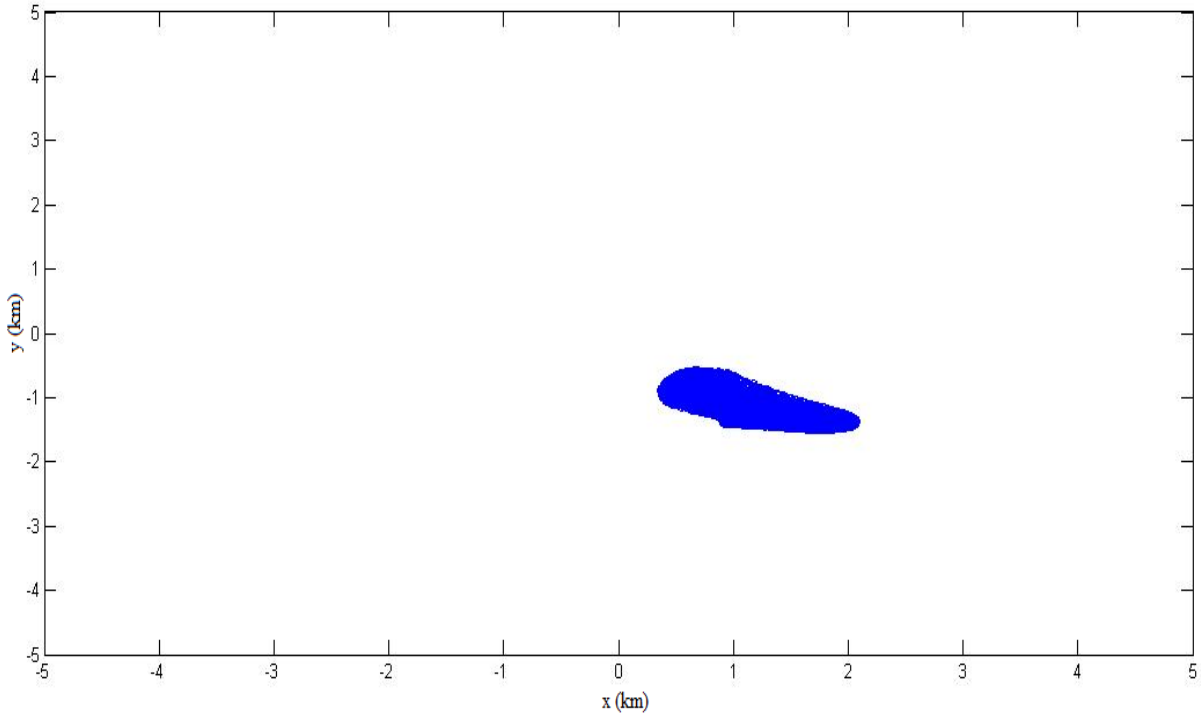
Time = 50 unit



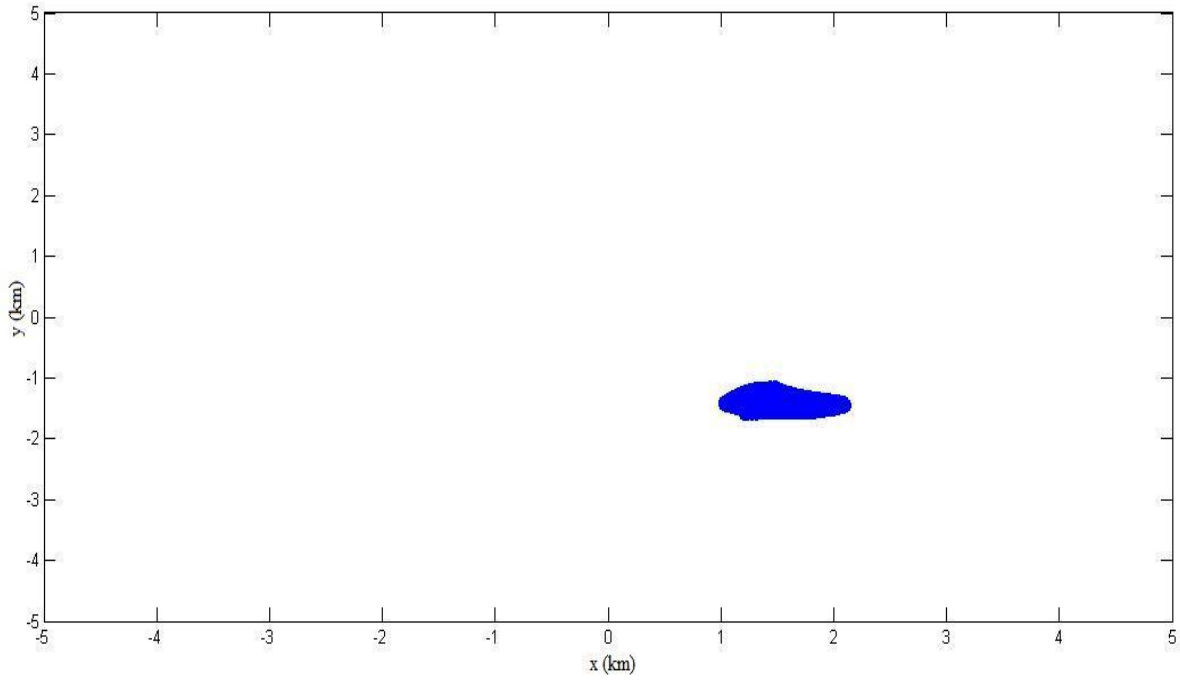
Time = 60 unit



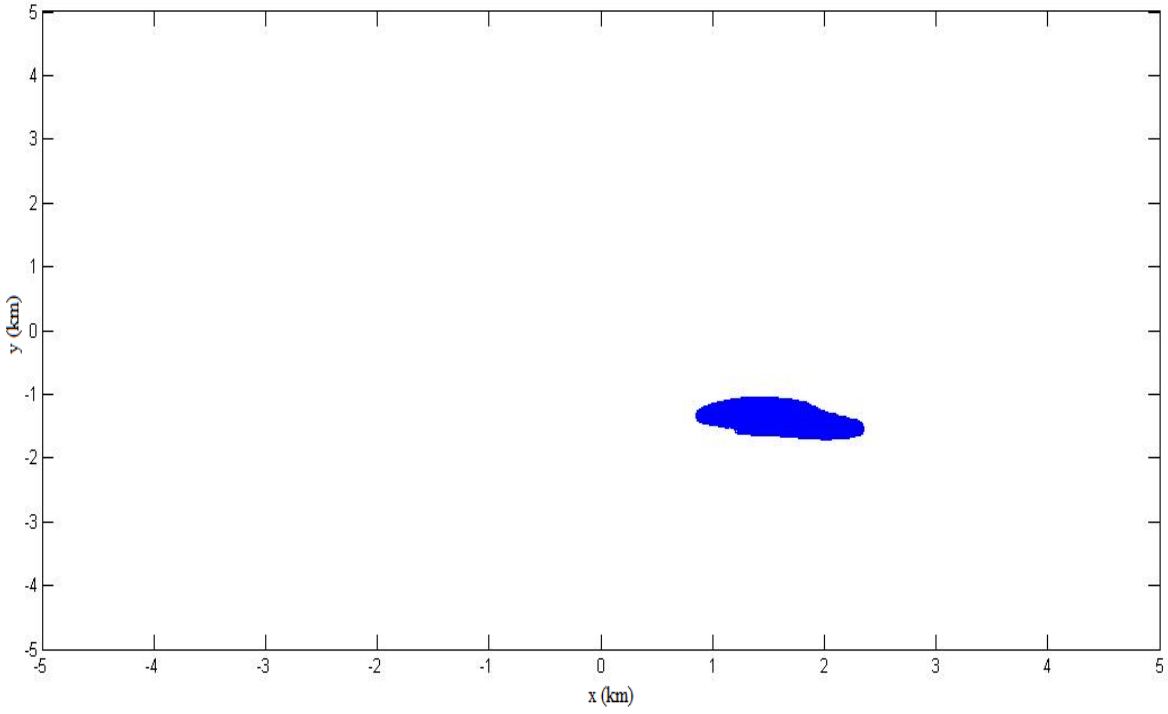
Time = 70 unit



Time = 80 unit



Time = 90 unit



Time = 100 unit

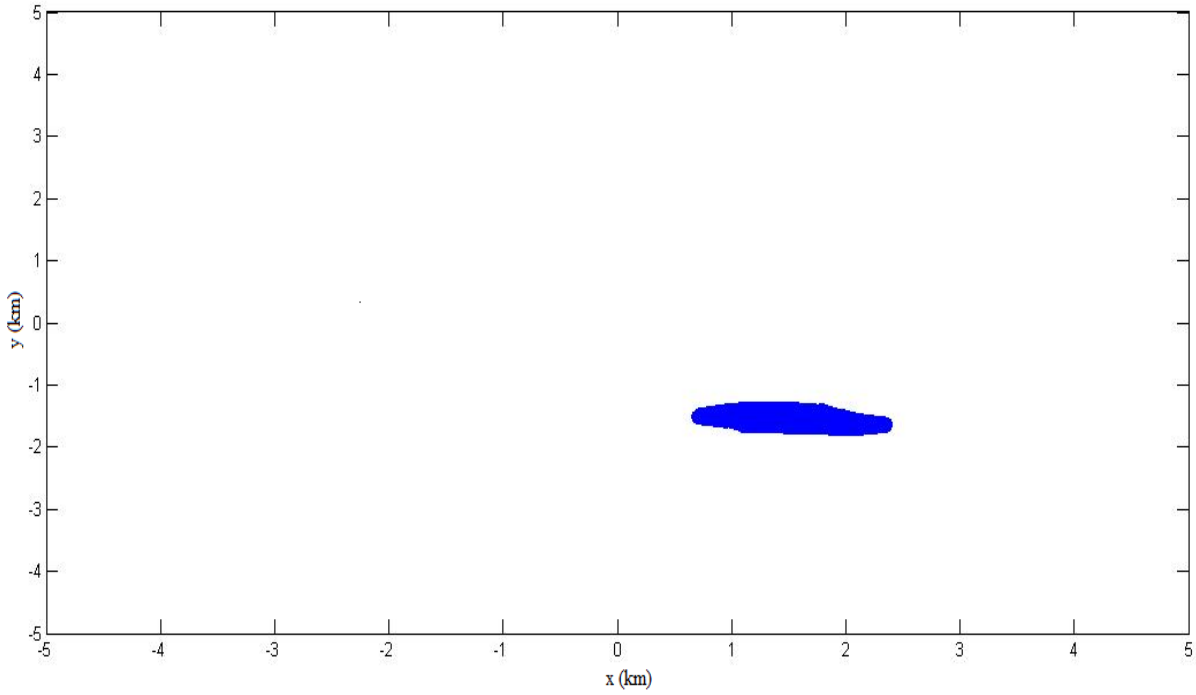


Figure 4.2 Positions of 6000 nodes that are randomly deployed in 0.5 km x 1 km area and moved in 3 days with meandering current mobility model.

As it can be seen from Figure 4.2, nodes are spanning kilometers in time which means that nodes are drifted away from its groups that should be considered by our key distribution scheme. This will be explained in the following section.

4.4 Key Establishment Phases

Key establishment can be examined in three phases: before deployment, after deployment and operational phases. First two phases are same as the nomadic mobility based model whereas the last phase is slightly different in meandering mobility based model.

Before Deployment phase is same as the nomadic mobility based model. Each surface buoy & underwater device unit is loaded with pairwise keys for the communications among surface buoys. Also each surface buoy & underwater device

unit is loaded with its groups' Blom key space. Public and private matrices (A and G matrices) of each group are loaded to the memory of owing surface buoy & underwater device unit. Each node is loaded with ID, a pairwise key for secure communication with its underwater device and a raw of its group's Blom Private Matrix (A). More details are explained in Section 3.4.1.

After deployment phase is also similar to the nomadic mobility based model. However underwater device is not rising or diving in meandering mobility based model. It is stable as model is two dimensional. Groups belong to same underwater device are deployed together. Also groups are deployed near to its owing underwater devices. After deployment each node finds its neighbors and tries to communicate with them securely. If they belong to same group, they communicate with Blom's key. If neighbor node belongs to another group which is owned by the same underwater device, then they establish a key with the help of their underwater device. If neighbor node belongs to another group which is owned by a different underwater device, they establish a link via their underwater devices. These are explained in detail in Section 3.4.2.

After key establishment phase is completed, nodes start to move according to meandering current mobility model. Underwater devices periodically sense their range to determine which nodes are drifted away and which nodes are include into range. If a node is broken away from its group then underwater device provides this node to be added to the nearest group. This operation's details are explained in 3.4.3. The difference in phases of meandering current mobility model with respect to phases of nomadic mobility model is occurred in changing the places of surface buoys during the simulation. As meandering current mobility model spans kilometers and the area is not limited, all the area need to be sensed during the simulation. However it is not possible to cover entire area with surface buoys and underwater devices due to its cost. As nodes are drifted away after a while, some surface buoys will not have any groups around themselves whereas some additional surface buoys are needed for new places of drifted nodes. For this reason, the redundant surface buoys are transported to new places where nodes are drifted and new surface buoys are needed.

4.5 Implementation Details

This model's simulation is implemented on Visual Studio 2010 environment and used C# for coding. In this simulation there are 200 groups where each group has 30 nodes. 6000 nodes are initially deployed in 0.5 km x 1 km area and simulation area is not restricted. There are 50 surface buoys and underwater devices which are moved during the simulation. Sensor range is 0.05 km [53]. Also similar to the simulation of nomadic mobility model, average energy consumption per packet is 70 milijoule [54] and energy consumption for encryption and decryption operations are 1.62 μjoule/byte and 2.49 μjoule/byte respectively [56]. According those values we performed our simulations for meandering mobility based model.

4.6 Performance Evaluation

Simulations are performed to get results for the metrics such as secure connectivity, resiliency and energy consumption. Time unit is determined as 0,03 day as it was performed in meandering mobility stream function. Total simulation time is $100 * 0{,}03 = 3$ days. Performance of the meandering mobility based model according to those metrics are illustrated and explained in following subsections.

4.6.1 Secure Connectivity

Secure connectivity illustrates the probability of two neighbor nodes' sharing common key. If it is 1.0 it means that all nodes in network can communicate with their neighbors. Then if this metric is nearly 1.0, then it shows that scheme is qualified. Figure 4.3 shows the graph of secure connectivity for meandering mobility based key distribution model.

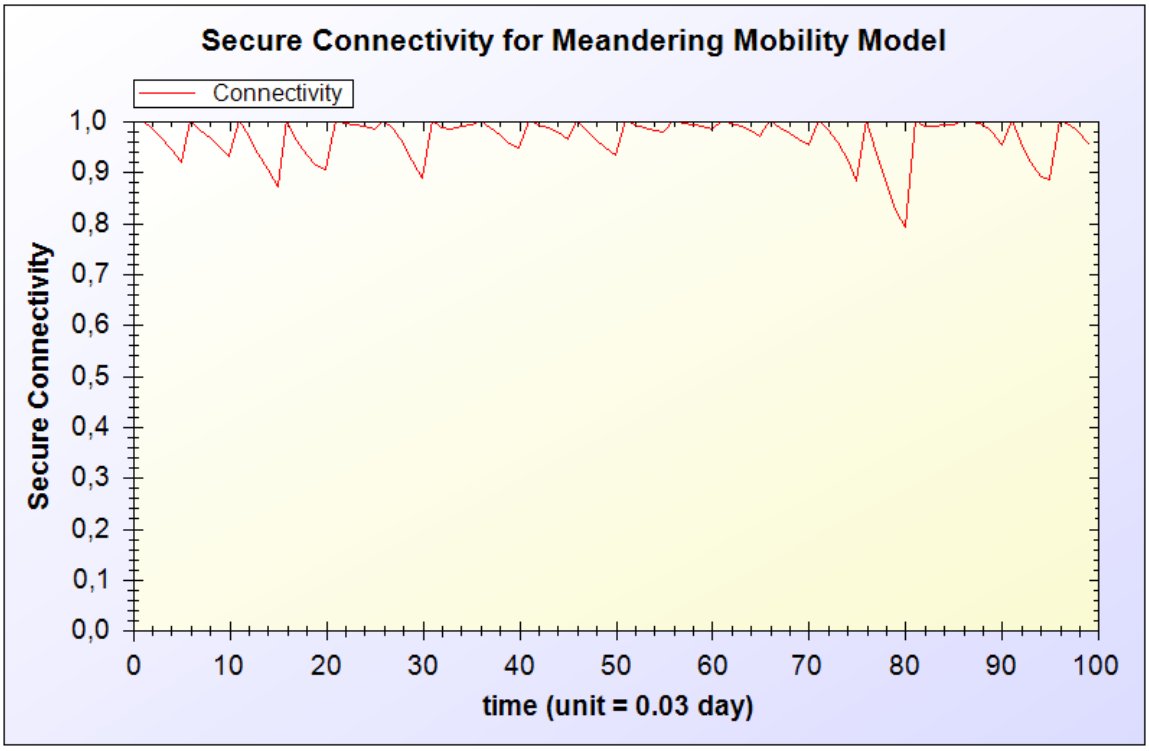


Figure 4.3 Secure connectivity for meandering mobility based model

As it can be seen from figure 4.3, connectivity fluctuates over time. Because of mobility, after a while nodes are dragged and start to drift away from its group. Then drifted nodes cannot communicate with their new neighbors due to the fact that they do not share any common keys with them. This is the reason for the decreases in the graph. However, underwater devices come to the help of the system and heal it. By the help of underwater devices, drifted nodes are connected to new neighbor groups and they start to communicate with those new nodes via new keys. In this way connectivity increases to 1.0.

4.6.2 Resiliency against Node Capture Attacks

Resiliency of the scheme against node capture attacks is measured by the following metrics: additionally compromised link ratio and total compromised link ratio. As it is explained in 3.6.2, when nodes are captured by the attacker, he can also reach the keys and the links of these nodes. If captured keys are used in another place of the network then the attacker also compromises these additional links. In order to measure this, additional compromise links ratio is used (additional compromised links/

all links). For the purpose of evaluating attacker's overall activity, we measure total compromised links ratio (total compromised links/all links). Total compromised links is the sum of additional compromised links and the links of captured nodes. Figure 4.4 and 4.5 show our scheme's performances.

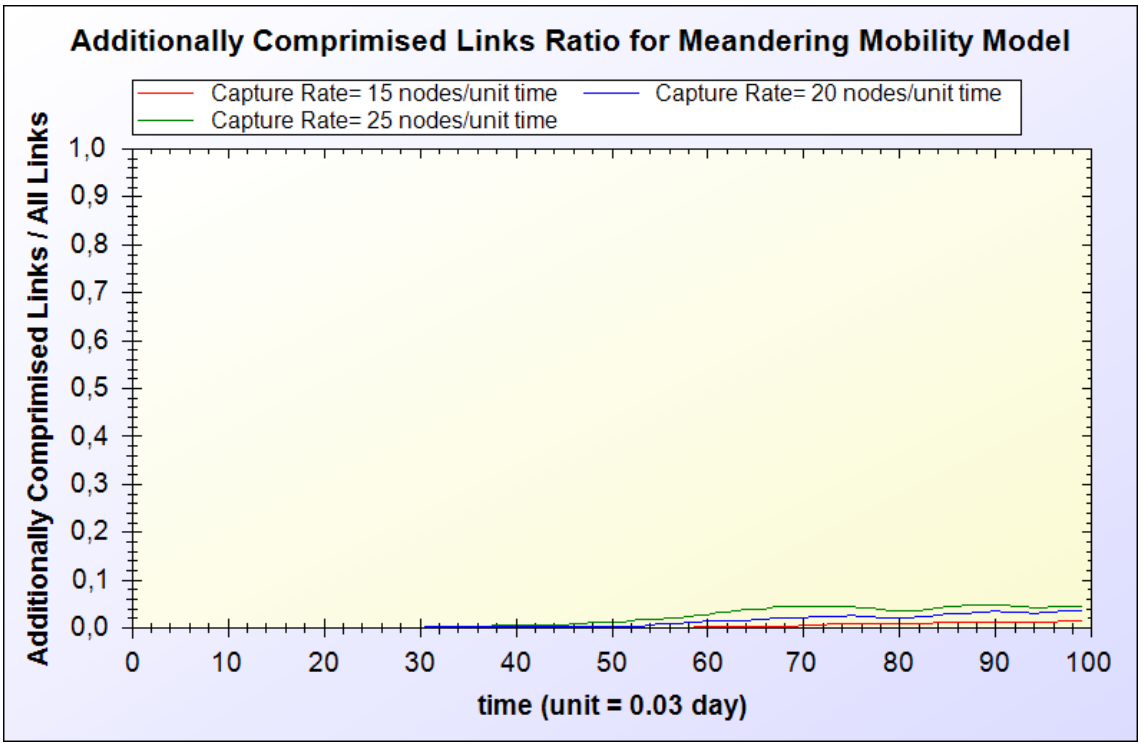


Figure 4.4 Additionally compromised links ratio for meandering mobility based model

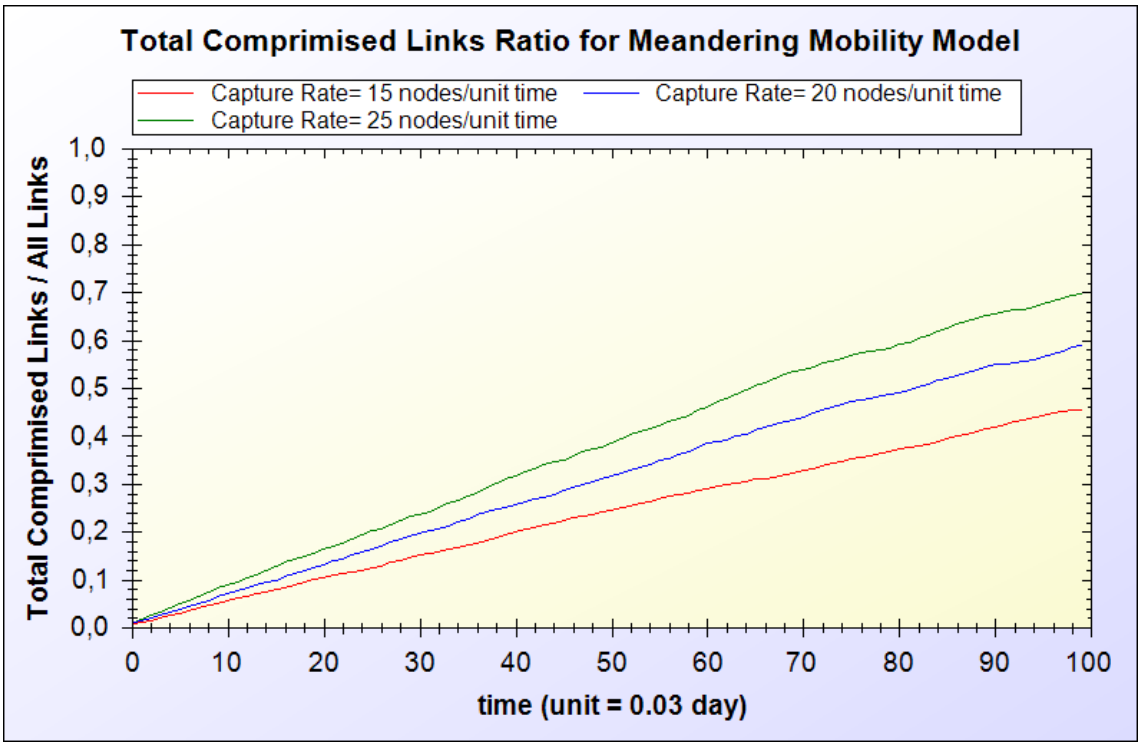


Figure 4.5 Total compromised links ratio for meandering mobility based model

In our system we used Blom's scheme for key distribution, which mean that all groups have λ-security. If captured number of nodes from a group exceeds λ, then attacker learns all the keys in the group, otherwise he cannot compromise any additional links. This can be seen in Figure 4.4. In this simulation node per group is 30 and λ is 10. Capture rate is determined as 15, 20 and 25 nodes per time unit. It is obvious that when 15 nodes are captured per unit time, additionally compromised links are nearly 0. If we increase capture rate to 20 nodes/unit time and 25 nodes/unit time, then simulation has perfect resiliency for a long time at the beginning of the simulation. After a while, the number of captured nodes of some groups exceeds λ, however it affects resiliency slightly and stays in reasonable level of 0,02. According to Figure 4.5, as it is expected, total number of captured links ratio increases when capture rate increases. When attacks power increases to 25 nodes/unit time capture rate, approximately 70% of links are captured.

4.6.3 Average Energy Consumption

In our simulations we measure energy consumption for key distribution. As nodes are battery-limited devices, it is important to have less energy consumption. We measure average battery consumption for the nodes at each instant of time. Communication between nodes and underwater devices are calculated to measure the battery consumption. Each packet is encrypted with AES which consumes 1.62 µjoule/byte, and decrypted with AES which consumes 2.49 µjoule/byte. Also each packet (64 bytes) transmission consumes 70 milijoules. In view of those values Figure 4.6 shows the average energy consumption per node for meandering mobility based model. Nodes do not separate from each other after unit time 40. For that reason, there is no need for fix up operation which results in no energy consumption. At the end of the simulation average energy consumption per node is converges to approximately 1250 milijoule.

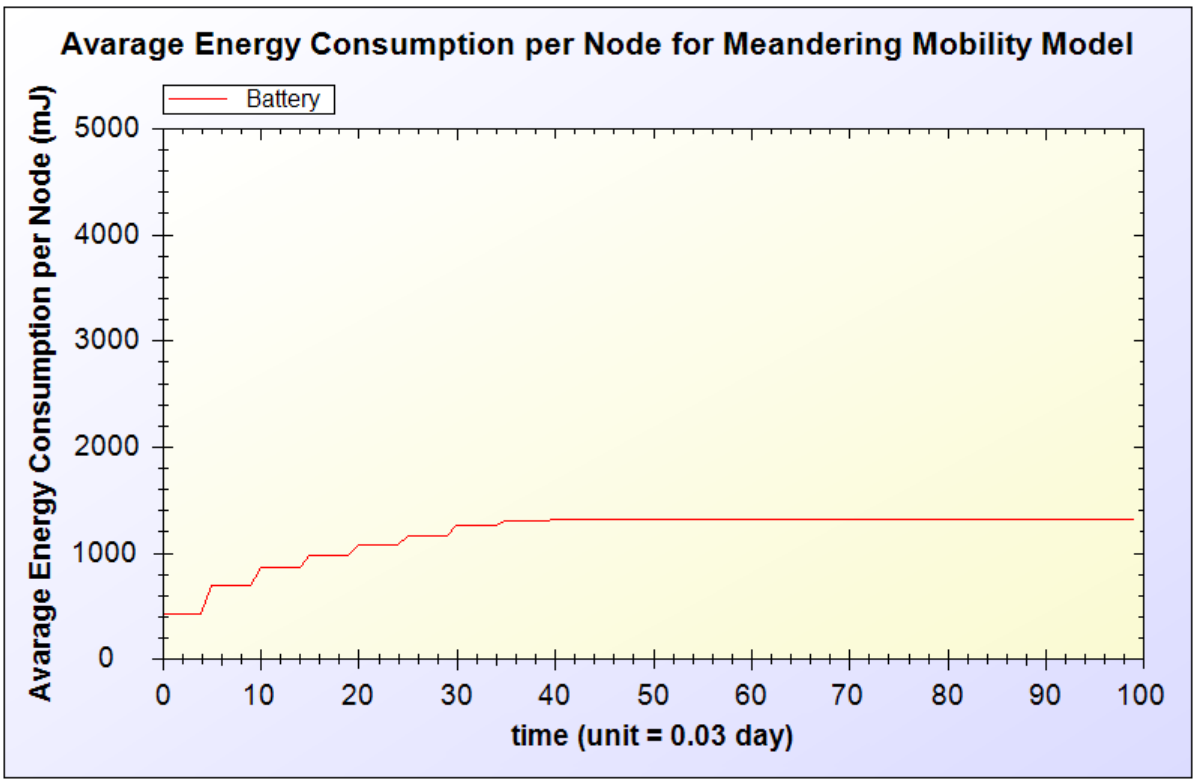


Figure 4.6 Average energy consumption per node for meandering mobility based model

4.6.4 Comparison with a Baseline Scenario

In our meandering mobility based model, since some part of the communication is airborne, communication cost is decreased. In previous section we illustrate our model's energy consumption performance. In this section we also want to compare our model with a baseline scenario. In this scenario, all communication is in underwater, airborne communication is not utilized. Communication packets are transmitted hop by hop through nodes. We did not use formal routing; instead packets are hopped in determined distances. In Figure 4.7, average energy consumption per node for baseline scenario for 20 meters /hop , for 40 meters/hop and our model are illustrated. As it can be seen if all the communication is done in underwater it will be much more costly. Also if the distance for each hop is decreased, average energy consumption per node is increased. The reason for this is more nodes are active to transfer the packet if distance per hop is decreased.

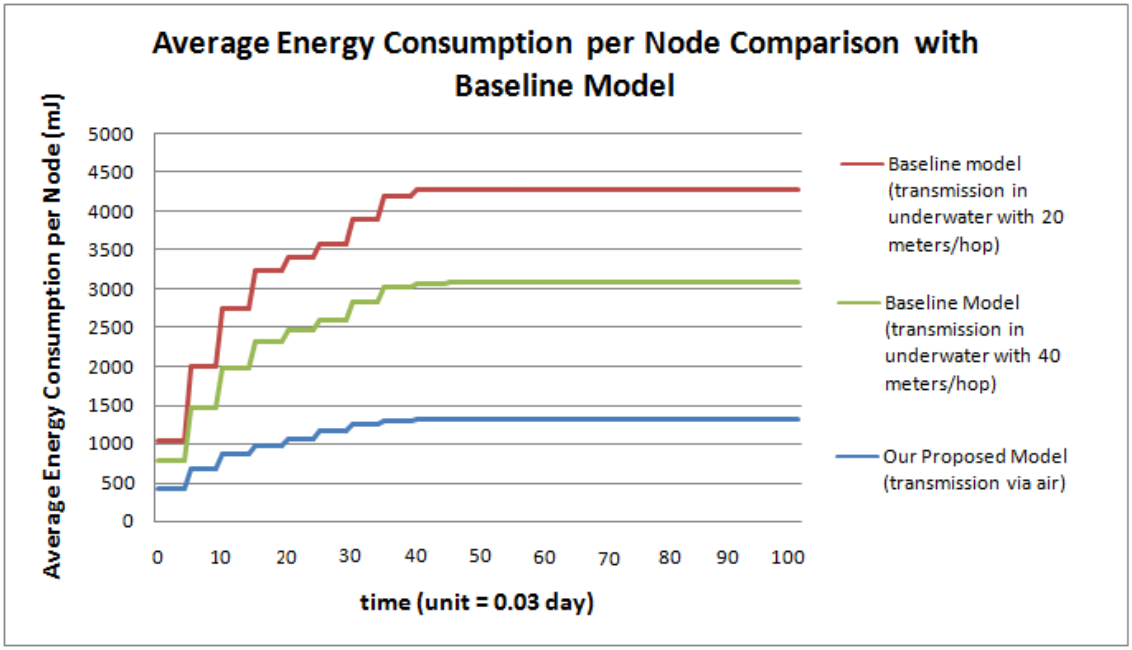


Figure 4.7 Average energy consumption per node comparison with baseline model

4.6.5 Memory Requirements

Since in proposed models Blom's scheme is utilized, memory requirement for meandering mobility based model is also similar to nomadic mobility model. As it is also explained in Section 3.6.4, each node is loaded with its own ID, owing underwater device' ID, a row of the private matrix A which has $\lambda + 1$ elements, seed s for the generation of the public matrix and modulation number of q. The length of these values is the length of symmetric key which we assume it is 128 bits. Then total requirement is $(\lambda + 5)x\ 128$. Since in our simulation, $\lambda = 10$, then total memory requirement is 240 bytes.

Chapter 5

Conclusions

In this thesis, we proposed a key distribution scheme for underwater mobile sensor networks. We applied key distribution scheme for two mobility models.

In Chapter 3, we introduce our key distribution scheme based on nomadic mobility model. This scheme is specialized for limited area in seashores. It is a three dimensional model with hierarchical structure that consists of group of nodes. We used Blom's key distribution scheme for each group. We have also performed analysis for connectivity and resiliency. Secure connectivity is approximately 1.0 since the system heals itself by the help of the structure of the scheme. It also has approximately perfect resiliency for a long time at the beginning of the simulation. After a while, additional compromised links ratio slightly increases; however, it does not exceed 0.1 which shows that our system is very resilient to node capture attacks. Average energy consumption is also low, which is approximately 400 milijoule at the end of the simulation.

In Chapter 4, we adopted our key distribution model based to meandering mobility model. This mobility model is more realistic, since it depends on the movement of the ocean. This scheme is for large areas in kilometers. This scheme is a two dimensional model and has hierarchical structure. Blom's key distribution scheme is also used for this scheme too. We performed simulations to evaluate metrics such as connectivity and resiliency. According to the structure of the system, secure connectivity pattern has zigzags. Due to the mobility, secure connectivity decreases in time. However with the help of fixing property of our scheme, secure connectivity reaches to perfect connectivity rapidly. In other words, our system heals itself. Besides, additionally compromised links analysis show that our scheme is highly resilient to node capture attacks since it does not exceed 0.1. Also, average energy consumption analysis shows that energy consumption is low, which is approximately 1250 milijoule at the end of the simulation.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422,

[2] Y. Cheng and D. P. Agrawal, “An improved key distribution mechanism for large-scale hierarchical wireless sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 35–48, 2007.

[3] D.P. Agrawal, Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole Publishing, 2003.

[4] N. Jain, D.P. Agrawal, Current trends in wireless sensor network design, International Journal of Distributed Sensor Networks 1 (1) (2005) 101–122.

[5] D. W. Carman, P. S. Kruus, B. J. Matt, Constraints and approaches for distributed sensor network security, NAI Labs Technical Report #00-010, September 2000.

[6] J.H. Cui, J. Kong, M. Gerla, S. Zhou, The Challenges of Building Scalable Mobile Underwater Wireless Sensor Networks for Aquatic Applications, IEEE Network, (0890-8044), 12-17, May/June 2006.

[7] J.Llor, M.P.Malumbres, "Modeling Underwater Wireless Sensor Networks", Wireless Sensor Networks: Application-Centric Design, Ed. InTech Education and Publishing, pp. 185-203.

[8] A. Mahdy and J. Groenke, “Target Tracking in Marine Wireless Sensor Networks,” International Journal on Advances in Networks and Services, Vol. 3, Issue 1, 2010.

[9] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless sensor network security - a survey”, Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, 2007.

[10] Y. Cheng, D.P. Agrawal, "Improved Pairwise Key Establishment for Wireless Sensor Networks," wimob, pp.442-448, 2006 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2006.

[11] H. Cam, S.Ozdemir, D. Muthuavinashiappan, P. Nair, "Energy efficient security protocol for wireless sensor networks,"Vehicular Technology Conference, 2003.

VTC 2003-Fall. 2003 IEEE 58th , vol.5, no., pp. 2981- 2984 Vol.5, 6-9 Oct. 2003 doi: 10.1109/VETECF.2003.1286170.

[12] S. Bandyopadhyay, E. Coyle, An energy efficient hierarchical clustering algorithm for wireless sensor networks, in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, California, April 2003.

[13] A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks", Elsevier Sci, J. Computer Communications, Vo1.30, 2007, pp. 2826-2841.

[14] B. Deosarkar, N. Yadav and R.P. Yadav, "Clusterhead Selection in Clustering Algorithms for Wireless Sensor Networks: A Survey" , In Proc. Int. Conf. Computing, Communication and Networking (ICCCN 2008), Dec. 18-20, 2008, Karur, Tamilnadu, India.

[15] V. Chandrasekhar,et al, "Localization in underwater sensor networks: survey and challenges," WUWNet, pp.33-40, 2006.

[16] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, November 2002.

[17] H. Chan, A. Perrig, D. Song, Random key pre-distribution schemes for sensor networks, in: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, California, May 11–14 2003, pp. 197–213.

[18] D. Liu, P. Ning, Improving key pre-distribution with deployment knowledge in static sensor networks, in: ACM Transactions on Sensor Networks (TOSN), 2005.

[19] D. Liu, P. Ning, W. Du, Group-based key pre-distribution in wireless sensor networks, in: Proceedings of 2005 ACM Workshop on Wireless Security (WiSe 2005), September 2005.

[20] R. Blom, An optimal class of symmetric key generation systems, in: Thomas Beth, Norbert Cot, Ingemar Ingemarsson (Eds.), Advances in Cryptology: Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, vol. 209, Springer-Verlag, 1985, pp. 335–338.

[21] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA,October 27–31, 2003, pp. 42–51.

[22] W. Du, J. Deng, Y. Han, S. Chen, P. Varshney, A key management scheme for wireless sensor networks using deployment knowledge. In Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'04), vol. 1, IEEE Computer Society, Los Alamitos, CA, USA, 2004, pp. 586–597.

[23] C. Castelluccia, A. Spognardi, RoK: a robust key pre-distribution protocol for multi-phase wireless sensor networks, in: Proceedings of the Third International Conference on Security and Privacy in Communications Networks (SecureComm'07), IEEE Computer Society, Los Alamitos, CA, USA, 2007, pp. 351–360.

[24] K. Kalkan, S. Yilmaz, O. Yilmaz, A. Levi, A highly resilient and zone based key pre-distribution protocol for multiphase wireless sensor networks, in: Proceedings of the Fifth ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'09), ACM, New York, NY, USA, 2009, pp. 29–36.

[25] S. Zhao, K. Tepe, I. Seskar, D. Raychaudhuri, Routing protocols for self-organizing hierarchical ad hoc wireless networks, in: Proceedings of IEEE Sarnoff 2003 Symposium, 2003.

[26] P. Gupta, P.R. Kumar, The capacity of wireless networks, IEEE Transactions on Information Theory 46 (2) (2000) 388–404.

[27] B. Liu, Z. Liu, D. Towsley, On the capacity of hybrid wireless networks, in: Proceedings of IEEE Infocom 2003, San Francisco, CA, April 2003.

[28] G. Jolly, M. C. Kusçu, P. Kokate, M. F. Younis: A Low-Energy Key Management Protocol for Wireless Sensor Networks. ISCC 2003: 335-340.

[29] T. Camp, J., Boleng, V., Davies, A survey of mobility models for AD hoc network research. In *Wireless Communications & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, no. 5, pp. 483-502, 2002.

[30] C. Bettstetter, Mobility Modeling, Connectivity, and Adaptive Clustering in Ad Hoc Networks. Utz Verlag, 2004.

[31] C. Bettstetter, H. Hartenstein, and X. Perez-Costa, "Stochastic properties of the random waypoint mobility model," Wireless Networks, vol. 10, no. 5, pp. 555–567, 2004.

[32] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in INFOCOM 2003, 30 March-3 April 2003, pp. 1312–1321.

[33] A. Caruso, F. Paparella, L.F.M. Vieira, M. Erol, and M. Gerla, The Meandering Current Mobility Model and its Impact on Underwater Mobile Sensor Networks. In Proceedings of INFOCOM. 2008, 221-225.

[34] J. Pedlosky, Ocean Circulation Theory. Heidelberg: Springer-Verlag,1996.

[35] G. G. Xie and J. Gibson. A Networking Protocol for Underwater Acoustic Networks. In Technical Report TR-CS-00-02, Department of Computer Science, Naval Postgraduate School, December 2000.

[36] J. Proakis, E.M.Sozer, J. A. Rice, and M.Stojanovic. Shallow Water Acoustic Networks. IEEE Communications Magazines, pages 114–119, November 2001.

[37] I. F. Akyildiz, D. Pompili, and T. Melodia. Challenges for Efficient Communication in Underwater Acoustic Sensor Networks. ACM SIGBED Review, Vol. 1(1), July 2004.

[38] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li. Research Challenges and Applications for Underwater Sensor Networking. In IEEE Wireless Communications and Networking Conference, Las Vegas, Nevada, USA, April 2006.

[39] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin, and P. Corke, "Data collection, storage, and retrieval with an underwater sensor network," in SenSys'05, San Diego, California, USA, 2005, pp. 154–165.

[40] A. Syed and J. Heidemann, "Time synchronization for high latency acoustic networks," in Proc. of Infocom, Barcelona, Spain, April 2006, pp. 1–12.

[41] V. Chandrasekhar, W. K. Seah, Y. S. Choo, and H. V. Ee, "Localization in underwater sensor networks: survey and challenges," in WUWNet '06, Los Angeles, CA, USA, 2006, pp. 33–40.

[42] D. Pompili and T. Melodia, "Three-dimensional routing in underwater acoustic sensor networks," in PE-WASUN '05: Proc. of the 2nd ACM Int. workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, Montreal, Quebec, Canada, 2005, pp. 214–221.

[43] P. Xie, J. Cui, and L. Lao, "Vbf: Vector-based forwarding protocol for underwater sensor networks," in In Proc. of IFIP Networking'06, Portugual, May 2006, pp. 1216–1221.

[44] N. Chirdchoo, W.-S. Soh, and K. C. Chua, "Aloha-based mac protocols with collision avoidance for underwater acoustic networks," in INFOCOM 2007, Anchorage, Alaska, USA, May 2007, pp. 2271–2275.

[45] D. Makhija, P. Kumaraswamy, and R. Roy, "Challenges and design of mac protocol for underwater acoustic sensor networks," in 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Boston, Massachusetts, USA, 03-06 April 2006, pp. 1–6.

[46] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," in WUWNet'06, Los Angeles, CA, USA, 2006, pp. 17–24.

[47] J. Kong, J. Cui, D. Wu, and M. Gerla, "Building underwater adhoc networks and sensor networks for large scale real-time aquatic applications," in IEEE MILCOM, Atlantic City, NJ, USA, 2005.

[48] P. Xie et al., "Aqua-Sim: An NS-2 Based Simulator for Underwater. Sensor Networks," in Proc. MTS/IEEE Oceans, Biloxi, Oct. 2009.

[49] Z. Zhou, J.-H. Cui, and S. Zhou, "Localization for large-scale underwater sensor networks," in UCONN CSE Technical Report:UbiNet-TR06-04, 2004.

[50] M. Erol, L. Vieira, et al, "Localization with Dive'N'Rise (DNR) beacons for underwater acoustic sensor networks," Proceedings of ACM International Workshop on Underwater Networks , Sep 2007.

[51] K. Chen, Y. Zhou, and J. He, "A localization Scheme for Underwater Wireless Sensor Networks," in Int'l Journal of Adv. Sc. and Tech. 4, 9-16, 2009.

[52] M. Ren, J. Jaworski, K. Rybarczyk, Random key predistribution for wireless sensor networks using deployment knowledge, 8th Central European Conference on Cryptography (2008).

[53] Dhurandher, S.K.; Khairwal, S.; Obaidat, M.S.; Misra, S.; , "Efficient data acquisition in underwater wireless sensor Ad Hoc networks," Wireless Communications, IEEE , vol.16, no.6, pp.70-78, December 2009 doi: 10.1109/MWC.2009.5361181.

[54] J.-H. Cui, P. Xie, H. Yan, T. Hu, Z. Shi, Y. Fei, S. Zhou, Z. Zhou, and Z. Peng, "Aqua-sim: An ns-2 based simulator for underwater sensor networks," in Proc. of IEEE OCEANS '09, Biloxi, MS, 2009.

[55] C . Detweiller, I. Vasilescu, and D. Rus, "An underwater sensor network with dual communications, sensing, and mobility," presented at Oceans 2007—Europe, Aberdeen, pp. 1–6 (2007).

[56] A. Wander, N. Gura, H. Eberle, V. Gupta and S Shantz, Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks, In IEEE International Conference on Pervasive Computing and Communication 2005 (PerCom '05), pp. 324{328, IEEE Computer Society, 2005.