SECURITY IN PERVASIVE HEALTH CARE USING LOCATION-BASED KEY GENERATION SCHEMES

A THESIS IN
Computer Science

Presented to the Faculty of the University
of Missouri-Kansas City in partial fulfillment of
the requirements for the degree

MASTER OF SCIENCE

by
DEBARGH ACHARYA

B.S. Uttar Pradesh Technical University-Lucknow, 2006

Kansas City, Missouri
2011

SECURITY IN PERVASIVE HEALTHCARE USING LOCATION-BASED KEY GENERATION SCHEMES

Debargh Acharya, Candidate for the Master of Science Degree

University of Missouri- Kansas City, 2011

ABSTRACT

Remote health monitoring has tremendous potential to improve quality of health care services in modern and ubiquitous medical environments. It helps to cut the cost in modern healthcare by avoiding unnecessary hospital visits for frequent checkups. In this context, security and protection of sensitive medical data such as Electronic Health Records (EHR), data integrity and protection of patient's privacy to be monitored are important aspects in order to increase user's acceptance of these new technologies. Secure communication protects data from unauthorized users and usually requires pair-wise keys. In all existing schemes these keys are generated and distributed to nodes wishing to communicate. The key generation phase is usually well-secured but the key distribution is not, as a result, they are vulnerable to security threats.

In this work, we investigate the key distribution problem inside a Body Sensor Network (BSN) and present two secure communication schemes which, unlike others, do not store a key chain in the memory from a universal key space and eliminate key

broadcast. We have made the key generation phase relatively more secured with the use of location information.

Authentication of biosensor nodes is also an important issue and has been taken into consideration in our schemes. Simulation of our schemes illustrates that they outperform some existing schemes and comparatively incurs less transmission and storage cost.

APPROVAL PAGE

The faculty listed below, appointed by the Dean of School of Computing and Engineering, have examined a thesis titled “Security in Pervasive Health Care Using Location-Based Key Generation Schemes” presented by Debargh Acharya, candidate for the Master of Science degree, and hereby certify that in their opinion it is worthy of acceptance.

Supervisory Committee

Dr. Vijay Kumar, Ph.D., Committee Chair
Department of Computer Science

Dr. Cory Beard, Ph.D.
Department of Computer Science

Dr. Yugyung Lee, Ph.D.
Department of Computer Science

CONTENTS

ILLUSTRATIONS

LIST OF TABLES

LIST OF ABBREVIATIONS

WWW	World Wide Web
WSN	Wireless Sensor Network
BSN	Body Sensor Network
BAN	Body Area Network
PHM	Pervasive Health Management
HIPAA	Health Insurance Portability and Accountability Act
EHR	Electronic Health Record)
ISO	International Organization for Standardization
DoS	Denial-of-Service
LH	Location-dependent Hash
LNH	Location-dependent Non Hash
IMD	Intelligent Medical Devices

ACKNOWLEDGEMENTS

I would like to express my appreciation to my advisor Dr. Vijay Kumar, without whom completion of this work would have been very difficult. I sincerely thank him for his assistance and constant guidance during the duration of my thesis and sparing time for my work whenever required. I thank him for allowing me to explore every possible aspect towards my work and guiding me at each and every step. I would also like to thank Dr. Cory Beard for his support towards my work and providing guidance whenever needed. I would like to thank Dr. Yugyung Lee for sparing some of her valuable time towards my work and ready to help me whenever I needed. It has been a privilege and a very good learning experience to work under all my committee members.

I would like to give a special thanks to my brother Dr. Debopam Acharya, my parents and friends without whose support and encouragement I would not have pursued my Masters, and completed successfully.

CHAPTER 1

INTRODUCTION

Wireless sensor networks (WSN) [1, 2] have made inroads to virtually every corner of our life and have received significant attention due to their widespread application in civilian and military operations. Recent advances in wireless communication and microelectronics have led to the development of low-cost and low-power sensor nodes. Sensors are inexpensive, low-power devices which have limited resources [2]. They are small in size, and have wireless communication capability within short distances. A sensor node typically contains a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter / receiver. A wireless sensor network (WSN) is composed of large number of sensor nodes with limited power, computation, storage and communication capabilities. Characteristics of a sensor network include flexibility in operation, high sensing fidelity, rapid and easy deployment, fault tolerance, low cost, dynamic changes and low maintenance.

Sensor networks have many applications in many fields, from medicine to military to inventory control. Some of the prominent applications in sensor network include:

- Traffic monitoring system: Traffic monitoring system monitors vehicle traffic on a highway, freeway or in a congested city area and provides information regarding accidents or traffic jams.
- Parking Monitoring System: Parking monitoring system provides identification of unoccupied parking spaces in busy city areas.

- Environment Monitoring System: An environment monitoring system detects and monitors environmental changes such as drought, floods and forest fires. It can also provide security in a shopping mall, parking garage, or other facilities.
- Battlefield Monitoring System: Battlefield monitoring system tracks enemy movements and deployments.
- Patient monitoring system: Inside a patient monitoring system biosensors or IMDs embedded in human body monitors blood pressure, body temperature, sugar level, heart beats etc.

1.1 Wireless Sensor Networks and Pervasive Healthcare

Since early 21st century, security and privacy [3, 4] in wireless sensor network has been an active field of research. Development of a robust security scheme is challenged by the limited capabilities of a sensor in terms of storage, processing power and energy. In today's modern and ubiquitous computing environments, it is important more than ever the necessity for deployment of pervasive healthcare architectures into which the patient is the central point who is surrounded by different types of small and embedded computing devices. These devices measures sensitive patient's medical data, physical indications and interacts with hospitals databases and therefore if required allows urgent medical response during emergencies and other critical situations. These environments should be developed incorporating the fundamental security requirements for real-time secure data communication, protection and confidentiality of sensitive medical data and measurements, data integrity and protection of the privacy of the patient being monitored.

1.2 Biomedical sensors or Intelligent Medical Devices (IMD)

Biomedical sensors take signals representing biomedical variables and convert them into an electrical signal. So it acts as an interface between a biologic and electronic signal.Biomedical sensors are classified into physical sensors and chemical sensors. Many different types of sensors are used in biomedical applications and are classified in Table 1.

Table 1. Characterization of Biomedical sensors

Physical Sensors	**Chemical Sensors**
Geometric	Gas
Mechanical	Electrochemical
Thermal	Photometric
Electric	Other physical chemical methods
Optical	
Hydraulic	Bioanalytic

Physical sensors measures muscle displacement, body temperature, blood pressure and flow, cerebrospiral fluid pressure, bone growth and density etc. While chemical sensors measures and detects chemical quantities by identifying the presence of compounds and monitors chemical activities in the body.

1.3 Need for Security in Pervasive Health Care

Medical information security of a pervasive health care system is very important as it is in any information system. In recent years EHRs have become more computerized and integrated among various healthcare providers. According to ISO, EHR (Electronic

Health Record) is any repository of patient data in digital form, stored and exchanged securely and accessible by authorized users. EHR is used in primary, secondary and tertiary health care by the staff of a general practice, a specialist facility upon referred by a primary care physician and by a team of specialists in a major hospital respectively.

Security is an important factor in medicine and health care [6] since patient's medical records must remain private. Inside a typical Body Sensor Network or Body Area Network (BSN-BAN) a biosensor or an IMD (Intelligent Medical Devices) gather sensitive medical information from a patient's body for transmission to a hospital and also provides medical services such as drug delivery or prosthetics to the patient being monitored. In accordance with the Health Insurance Portability and Accountability Act of 1996(HIPAA) all hospitals and clinical settings must ensure secrecy and privacy [8] of patients' medical information. Therefore any BSN-BAN which senses and measures various body parameters needs to ensure that the patient's medical data is never leaked or provided to unauthorized entities, either during the sensing or communication process.

A possible breach in security inside a BSN-BAN can lead a malicious entity to disguise as the controlling base-station and inject unwanted, false medical instructions such as a drug administration leading to catastrophic results such as patients' death. It is always a challenge to provide security in BSN-BAN. One reason is the wireless nature of the whole set up. Biosensors communicate between themselves and the base station using wireless communication so an eavesdropper can always listen to this communication, insert bogus messages or jam the communication. Another reason is the limited capability of biosensors such as reduced processing power and battery life. So the traditional

cryptographic algorithms cannot be used to secure the communication between these devices.

There are many security issues [3, 4, 5] regarding WSN-BSN-BAN.

- **Sensor node compromise:** This involves attacking, capturing and reprogramming a sensor node. Once attacker captures a few nodes, a variety of attacks are mounted by the adversary such as distortion of sensor data, exhausting the network by creating false routing loops and extracting secure information.
- **Eavesdropping:** Eavesdropping can be done where an adversary monitors transmissions of communication between nodes and gains important information.
- **Denial-of-Service (DoS) attacks:** DoS attacks aim to destroy network functionality rather than subverting it or using the sensed information and are extremely difficult to defend. Potential defenses against DoS attacks are as varied as the attacks themselves.
- **Malicious use of commodity networks:** The use of sensor networks will inevitably extend to criminals who can use them for illegal purposes. With widespread use, the cost and availability barriers that discourage such attacks will drop.

1.4 Thesis Overview

In this thesis the secure communication between biosensors are divided into three phases: *initialization or set up phase*, *secure key generation phase* and *medical data communication phase*. In our two schemes the biosensor nodes communicate with the parent node or head node *H* inside the BSN-BAN with wireless link. We have followed a *centralized approach* for our a) Location-dependent Hash (LH) chain based scheme and a

distributed approach (b) Location-dependent Non Hash (LNH) chain scheme. The two schemes proposed are analyzed and the comparisons with other similar schemes are presented along with the result of their implementation.

The thesis is organized as follows. Chapter 2 presents the preliminaries for the research. Chapter 3 presents our problem statement, followed by the description of our protocols in Chapter 4. Chapter 5 presents the mathematical analysis of the protocols, implementation results and security analysis. Chapter 6 presents the conclusion and future work.

CHAPTER 2

PRELIMINARIES

2.1 Evolution of Pervasive Health Management

Pervasive Health Management (PHM) mainly involves round-the-clock monitoring and collecting vital health information like pulse, temperature, blood pressure, blood glucose level, respiratory function and a variety of other physiological metrics with the help of portable biomedical devices and other Intelligent Medical Devices (IMD). This real time information may then be sent to health agencies and health practitioners for further analysis. This not only helps in self managing various chronic diseases like Heart Diseases, Asthma, Diabetes, etc, but also in preventive healthcare for persons of all ages. So far PHM has evolved in three stages till now [7]:

- The Stand-alone health monitors [8] are used to take readings manually and then stored manually or electronically.
- Hospital and Home based Tele-health monitors that capture data from wired medical devices that are wired to or around patient's body and transfer it to backend servers via landline phones.
- Pervasive Healthcare Management where a cell phone or PDA directly gathers or captures data 24/7 from various wireless biomedical sensors attached to human body and transfers them to backend servers wirelessly to be further processed for diagnosis and appropriate action. This is easier to use as the entire system is wireless and mobile.

PHM creates a win-win situation for everybody like patient, doctor, pharmaceutical companies, hospital and insurance agencies. A patient has peace of mind by being silently monitored all the time. Medical units such as doctors, specialists and nurses can be reached anywhere anytime who can diagnose and provide accurate medical advice since they have access to real time medical records. Hospital and pharmaceutical companies can extend their health care management programs effectively and insurance companies will save significant funds with reduced number of hospitalizations.

Today's social conditions are perfect for pervasive health monitoring because of high growth of chronic diseases and aged population, better penetration of mobile phone industry, and due to high medical expenses in hospitals. The market surveys have already shown that the costs with pervasive monitoring are several times less than the cost of monitoring at hospitals. Here is an example to further illustrate the advantage that involves symptoms common to the world population.

Example 1: Emily is a 15 year old who has just been diagnosed with juvenile diabetes. She uses a glucose meter and cell phone to monitor her blood sugar levels. The cell phone reminds Emily to check her blood sugar regularly during the day, and her glucose meter seamlessly transmits the measurements to his cell phone after each use. The data is transferred to a diabetic monitoring service that maintains Emily's long-term history and looks for abnormal events. If a reading is unusual, or if Emily skips a test, the system automatically contacts her parents/relatives, who can get in touch with her immediately.

2.2. Features of Pervasive Health Management

PHM has the following features:

- Pervasive health care is available anytime and anywhere.

- Disease monitoring 24/7 using wireless biomedical sensors.
- Medical data can be transferred for evaluation to a medical call center round-the-clock and feedbacks are given to patients or action is taken immediately in case of emergency.
- Data is stored in patient's medical history in the form of Electronic Health Record (EHR).
- For further analysis EHR can be sent to doctor / specialist in a hospital by email, fax, or on mobile on real time basis and remote consultations can be provided using e-mail, text, chat and video conferencing .
- Trend analysis and alerts can be provided to patients for overall improved disease management leading to greater life expectancy.

2.3. Socio-economic Reasons for PHM

In 2008, total healthcare spending in the USA reached $2.3 trillion which was 16% of the gross domestic product (GDP) [9]. In 2009, 145 million people or almost half of all Americans lived with a chronic condition [10]. In 2009, United States spent 85 percent of the health care cost on people with chronic conditions. Figure 1 shows information about US population with one or more chronic diseases [11].

By 2015, U.S. healthcare spending is expected to increase to $4.4 trillion, or 20% of GDP. Industry experts agree that the U.S. healthcare system is plagued with excessive administrative expenses, inefficiencies and inappropriate measures. These problems significantly increase the cost of medical care and health insurance for employers and consumers.

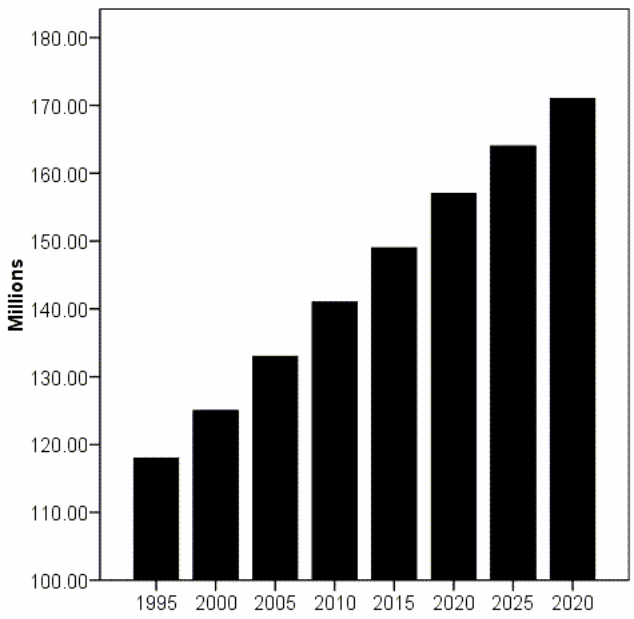

Figure 1. US population (in millions) with one or more chronic diseases.

In the year 2009, data from Center for Disease Control [12] show the observation on physician visits as given in Table 2. Based on the table we can infer that approximately 441.98 million visits were made to primary care physicians only for the purpose of performing general medical examination. A pervasive health monitoring system is expected to almost eliminate visits to a physician for general medical examination as the system monitors medical data round-the-clock, issues alerts in case of an emergency and recommends appropriate action. Assuming an average cost of $100 per visit translates to saving of approximately $ 44.19 billion in hospitals visits only. If we consider all the savings from hospital, pharmaceutical and insurance companies, the total costs savings will be much more significant.

Table 2. Physician visits observation data, 2009

Number of visits to a physician in USA	902 million
Number of visits to a physician per 100 persons	306.6
Percent of visits made to primary care physicians	49 per cent
Most frequent reason for visit	general medical examination
Average cost of hospital visit	$100.00
Approximate total savings to US healthcare using PHM	$ 44.19 billion

With researches predicting a shortage of 35,000 to 44,000 primary care physicians in the USA by 2025 [13] and approximately 0.8 million shortage of nurses (Figure 2) by 2020 [14], mobile health monitoring is going to get significant attention in healthcare management.

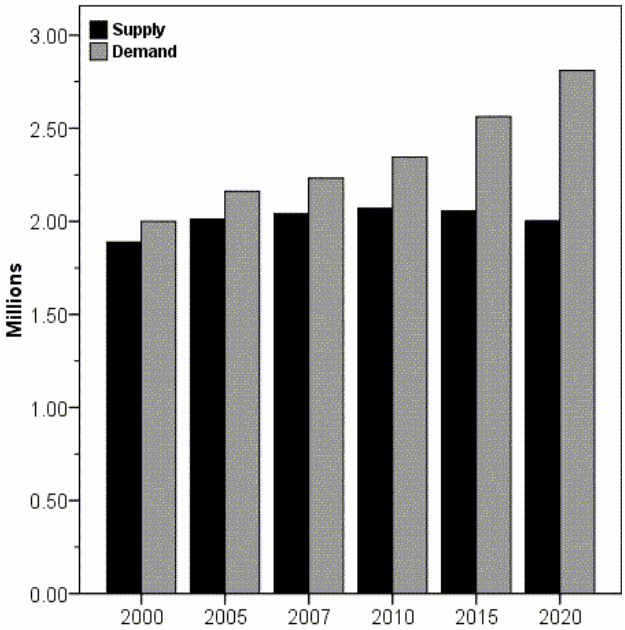

Figure 2. Demand and supply of nurses (in millions)

CHAPTER 3

PROBLEM STATEMENT

3.1 Problem Specification

Many applications in BSN-BAN involve secure communication among large numbers of wireless sensor devices. In order to protect sensitive medical data and sensor readings pair-wise keys should be used for encryption. In all existing schemes these keys are generated and distributed to nodes wishing to communicate. The key generation phase is usually well-secured because it is completed at system setup time, but the key distribution is vulnerable to security threats. The idea of key broadcast seems useful; however, in reality it is fairly unreliable [19], especially for devices with IEEE 802.15.4 radio packets, a de facto standard in WSN [2]. While the maximum broadcast packet size is a few kilobytes of payload, an individual 802.15.4 radio packet can carry a maximum of 128 bytes of data and this mode is inherently unreliable because the list of recipients is unknown. Datagrams broken into three or more fragments (over 200 bytes of payload) are almost likely to experience some loss. If that happens then the lost data must be retransmitted, and if required, may have to be fragmented and defragmented again, leading to further data loss and increased power consumption [25]. It is all the more important that the loss of data which is actually medical data in our case remains minimum or zero. Hence, schemes that transfer packets with subset of keys may lose a portion of data as they would be fragmented during broadcast. Important data should generally be transferred in unicast mode via radiograms or radio streams. For these

reasons we took a different approach for generating and using the keys for communication instead of distributing them to nodes wishing to communicate.

3.2 List of Possible Attacks

We have divided the possibility of attacks in a pervasive health care set up into patient's side and the caregiver side. Here is the list of some of the possible security issues.

Patient's Side:

- Probing attacks, tampering attacks by malicious users that have explicit interference and physical access to an IMD or a biosensor. A malicious node can prevent a legitimate warning generated by an IMD or a biosensor from reaching the appropriate authorities. Also it can generate a false warning for a patient leading to unwanted actions such as false diagnosis or a wrong drug delivery. This is a form of Active attack.
- Attacks in the form of eavesdropping by a malicious node into the communication link between an IMD and other systems. This is a form of passive attack.
- A malicious node can take advantage of the fact that biosensor devices are resource constrained and therefore can generate bogus messages inside the network leading to wastage of much needed battery life.
- The biosensors are implanted or attached to patient's body so another side effect of "overworking of biosensor nodes" is the problem of tissue heating. Due to prolonged exposure to abnormal temperatures can cause tissue degeneration leading to severe health problems such as leukemia.
- Attacks can also be made by insiders such as patient reporting false medical data.

Severe security lapses can occur at the Caregiver Side too such as:

- Security breach because of granting system access to improper persons, *"who gets access to what"*.
- Security breach because of not revoking terminated employee's access that are fired or retired.
- Security breach due to common errors such as "*Mailbox Full*" and important medical messages not getting delivered to required persons.
- Security breach due to improper configuration of hardware and software being used, *"never trust on defaults"*.
- Security breach due to Group Activities using a Group Login. Activities cannot be monitored in situations where a common login is being used to monitor a patient's medical information by a group of doctors and nurses.
- Security breach due to improper training.
- Security breach due to workstations not getting automatically locked when no one is around.

3.3 Related Work

Several works have discussed the problem of devising a secure mechanism for key generation and distribution [3, 15, 19, 20, 21, 30, 31]. Eschenauer and Gligor [16] proposed a probabilistic key pre-distribution scheme for pairwise key establishment. The main idea of this scheme was to let each sensor node randomly pick a set of keys from a universal key pool before deployment so that any two sensor nodes must have a certain probability of sharing at least one common key. We call this as the basic probabilistic key pre-distribution scheme or EG scheme. Chan et al. [17] further extended this idea and

developed two key pre-distribution techniques (a) *q-composite key pre-distribution* and (b) *random pairwise keys scheme*.

The q-composite key pre-distribution uses a key pool but requires two sensors to compute a pair-wise key from at least q pre-distributed keys which they share. This approach increases the amount of key overlap required for key-setup. Further, to preserve the probability of two nodes sharing sufficient keys to establish a secure link, it is necessary to reduce the size of the key pool. As a result, a small number of compromised nodes may affect a large fraction of pair-wise keys. The random pair-wise keys scheme randomly picks pairs of sensors and assigns each pair a unique random key. Both schemes although improve the security over the basic probabilistic key pre-distribution scheme, the pair-wise key establishment problem remains unsolved. In the basic probabilistic and the q-composite key pre-distribution schemes, as the number of compromised nodes increases, the fraction of affected pair-wise keys increases quickly. Although the random pair-wise keys scheme does not suffer from the above security problem, due to memory constraint nature of sensor nodes, the network size remains small.

Perrig et al. [5] proposed SPINS, a security architecture specifically designed for sensor networks. In this scheme each sensor node shares a common key with the base station. The base station acts as a trusted third party when two nodes establish a new key. Having base station as a mediator for new key generation is costly because of increased communication overhead.

Das et al. [30, 32] proposed a scheme which is an extension of Dong and Liu's scheme. The main idea is to deploy a small number of High end sensors (H-sensors)

together with a large number of Low end sensors (*L*-sensors). Before deployment the set up server stores id_s, master keys, n key plus id combination $K_{Hi,\ uj}$, id_{uj} (key and id combination of *H* and *L* sensors respectively) and the polynomial share (Blundo and Santis, 1993) of all *H* sensor into each *H* sensor. Also each *L* sensor are loaded with its own id, master key and *l* key plus id combination $K_{u,\ vj} = \text{PRF}_{MKvj(idu)}$ where u and v are *L* sensors, MK_{vj} is the master key of any sensor v_j and id_u is the id of sensor *u*. For common pairwise key generation, *H* and *L* sensor will broadcast their id_s to check whether the key ring of them contain the id of another node. If the id is found in its memory then the associated key becomes the secret pairwise key.

Du et al. [31] proposed a symmetric pre distribution (AP) key management scheme. Here in this scheme each *L* sensor is preloaded with *l* keys and *H* sensor are loaded with *M* keys where $M >> l$. For distributed pairwise key distribution each *L* sensor broadcasts its key id_s associated with the keys from its key ring to discover if they share a common key. For centralized pairwise key distribution each *L* sensors broadcasts its key id_s to its cluster heads (*H*). The key discovery is done by *H* as it has all the information in its memory so it can determine if two *L* sensors u and v are neighbors based on their location proximity and then a common key is allocated to each pair of neighboring *L* sensors. The approach is very similar to other pairwise key distribution schemes. This scheme suffers from cost overhead due to message transmission during pairwise key generation.

Recently location information [27, 33, 34] of sensor nodes has been used for key distributions. Liu and Ning [23, 24] proposed closest pairwise key scheme (CPKS) and closest polynomial key scheme (CPPS) for key generation and distribution. It is an extended version of random pair-wise key scheme. The main idea here is to have prior

deployment knowledge of the deployed sensor nodes. Here each sensor node share pairwise key with its *n* closest neighbors. The schemes lose their performance as the deployment error between actual and expected locations of the deployed sensor nodes increases. Das [34] extended the idea of Liu and Ning by proposing ECPKS (enhanced closest pairwise keys scheme). ECPKS used both pre deployment as well as post deployment knowledge for key pre distribution mechanisms.

Authentication of sensor node is also a major area of research while developing schemes for key generation and distribution. Perrig et al. developed a protocol named μTESLA [4] for broadcast authentication in distributed sensor networks. This protocol is a modified form of stream authentication protocol called TESLA [5]. μTESLA protocol uses a serial chain of authentication keys which are linked to each other by a pseudo random function [22]. This pseudo random function is a one way function. It achieves authentication by delayed key disclosure in the key chain. Liu et al. [23, 24] proposed a modified form of μTESLA. The main idea was to predetermine and then broadcast the key chain commitments instead of message transmission.

Zhang et al. [26] proposed a node-to-node neighborhood authentication scheme using LBKs (Location-based Keys). In this scheme each node has to broadcast its location to its neighboring nodes for authentication. Broadcasting of confidential entities such as location information possesses a security risk as discussed above.

3.4 Thesis Approach

Here we are proposing a pervasive health care system where our schemes can be implemented inside the BSN-BAN. Pervasive health care systems provide medical units specially doctors and nurses at a hospital with remote access to real-time patient's health

data. The whole medical system (figure 3) runs a large diversity of applications which consists of setting up communications among various implantable medical devices (IMDs) such as sensors, actuators and smart hand held portable devices (PDAs). Collection of medical data is done inside the BSN and then it is further integrated with patient's EHR through communication channels such as internet and other asynchronous transfer through cellular network. The messages and medical records are further processed and accessed by authorized doctors and specialized medical personnel on demand to give care and treatment to the patients.

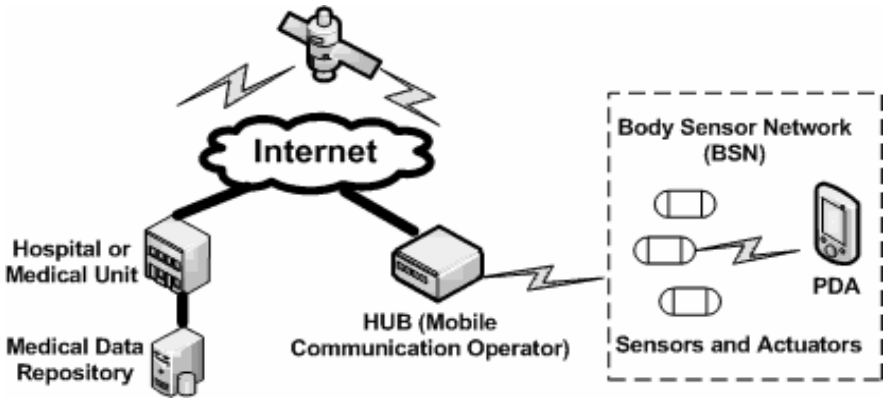

Figure 3. High level view of a pervasive health care architecture.

Inside the pervasive healthcare environment, resource-constraint BSN-BAN needs data transmission scheme that requires minimal cost in terms of memory and power usage. A typical sensor node when idle consumes less than 100 μwatts of power. A significant portion of power is used in data transmission with devices having data transfer speed of 10-250 kbps consuming about 30-40 mW of power. In several prominent key distribution schemes for BSN, data transmission involves broadcast of a subset of keys from a key pool. While broadcast involving IEEE 802.15.4 devices are unreliable as

indicated above, multiple broadcasts results in significant consumption of power. Also, as the size of program memory of a typical sensor may range from 4-128 kilobytes, storing a large subset of key ring sizes (in order of few hundreds) as discussed above may involve use of a significant portion of overall program memory. We present two schemes that eliminate the key distribution phase in setting up secured communication among sensor nodes. Thus, unlike most other schemes our schemes do not require sensor nodes to store a key chain in memory from a universal key space and broadcast them to other nodes. Instead, the individual and common pair wise keys are generated and undergo unicast in the network. We have exploited the strength of location information (x' and y' coordinates) in developing our scheme. An x'/y' value is unique and cannot be hacked without being identified.

BSN-BAN environment can be indoor or outdoor. For outdoor localization GPS is the most favored and used technology. But for indoor which is actually the environment for pervasive health care networks GPS technology is not feasible. Several indoor localization schemes have been proposed. For our set up we are using RFID tag based indoor localization mechanism [18]. In our schemes the sensor nodes communicate with the parent node or head node *H* inside the BSN-BAN with wireless link. We present (a) Location-dependent Hash (LH) chain based scheme and (b) Location-dependent Non Hash (LNH) chain scheme. The first scheme creates several hash chains and involves more computation for the head node. The second scheme does not create hash chains but involves more data storage in the head node.

CHAPTER 4

PROPOSED SOLUTION

4.1 The Implementation

In this work, we investigate the key distribution problem in body area networks and present two secure communication schemes which, unlike others, do not store a key chain in the memory from a universal key space and eliminate key broadcast. We have made the key generation phase relatively more secured with the use of location information. Authentication of sensor devices is also an important issue and has been taken into consideration in our schemes. Simulation of our schemes illustrates that they outperform some existing schemes and comparatively incurs less transmission and storage cost. Here is our software architecture in figure 4.

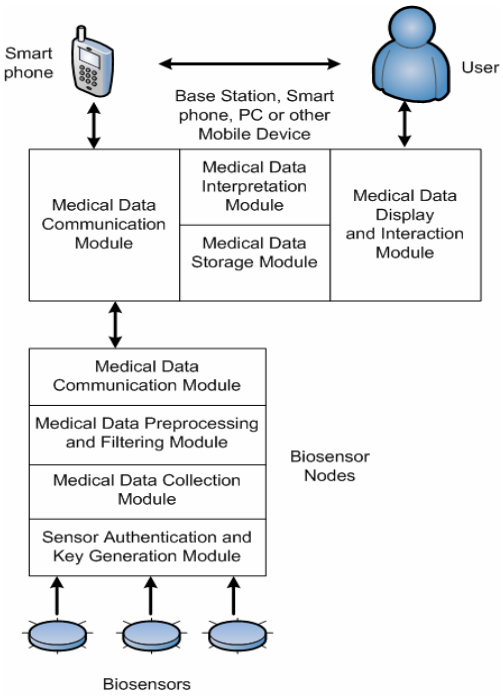

Figure 4. Software Architecture

4.2 Location-Based Hash (LH) Chain Scheme

This scheme uses location information (x' and y' coordinates) of sensor nodes first to generate the individual key sets which are then used to generate the common pairwise key between any two sensor nodes wishing to communicate. This approach makes sure that no two sensor nodes can have any keys in common.

The pairwise key generation scheme is divided into two steps: (a) deployment of sensors and individual key generation by nodes using (x'/y') and (b) authentication of sensor nodes and generation of pair wise key. Table 3 shows the notations we have used to describe the schemes.

Table 3. Notations Used in the Schemes

Notation	Meaning
A, B	Communicating Nodes.
H	Head node of a cluster.
ID_A, ID_B	Identifier of node A and B
$K_{A1}.... K_{A3}$	Key set for A generated by hash chain.
$K_{B1}.....K_{B3}$	Key set for B generated by hash chain.
K_{AB}	Common pairwise key for A & B.
Lat_H	Location information of head node, x' in this case
Lat_A	Location information of node A, x' in this case
K_A,K_B	Individual keys of node A and B respectively
LOC_A	Location information of node A, x'/ y' coordinate
LOC_B	Location information of node B, x'/ y' coordinate

4.2.1 Sensors Deployment and Hash Chain Formations

In this step the key is generated after deploying the sensors and forming the clusters. We can safely assume that this initial setup securely saves sensor ID together with location information (X'/Y') of all nodes in each head node prior to key generation and each sensor devices are capable of determining its location information using RFID tag based indoor localization mechanism [18] so the y can uniquely determine their own location. The scheme involves creating one way hash chains by hashing the location information to generate individual keys for each sensor nodes. All hash chains are generated using hash functions starting from the head node of a cluster. Figure 5 shows our scheme of using location information in hash chains to generate individual key rings. For simplicity we have consider x'= LAT (latitude information) and y'=LON (longitude information) or vice versa wherever required.

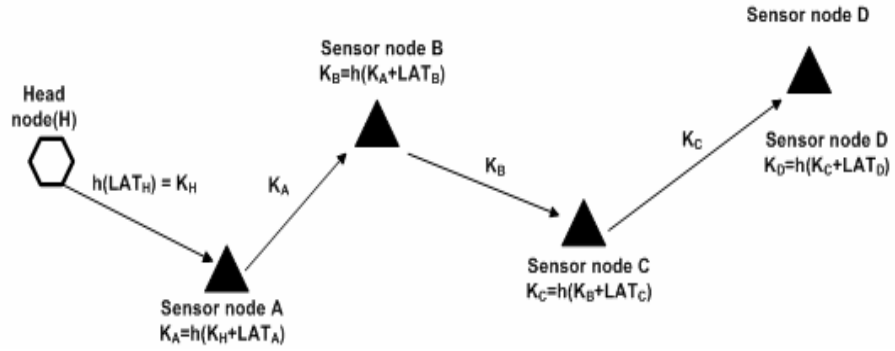

Figure 5. Hashing of Location Information for individual key generation

Thus, using a hash function h the head node (H) generates a hash value $K_H = h(Lat_H)$ by hashing its location information (x' and y' coordinates). It passes this hash value to the next neighboring node A which in turn generates K_A (key of A) by computing the hash of sum of K_H and its location information, Lat_A which is $K_A = h(K_H+Lat_A)$. Next, node A

sends K_A to its adjacent node and thus the individual key generation continues until the last node of the cluster has generated its key. In our scheme we require three keys in the key ring set of each sensor node which can be generated using x', y' and both. In the example above we have used the x' coordinate for generating these keys. It can be argued that two or more sensor nodes can have either x' or y' coordinate information same but it is impossible for both x' and y' information of one sensor node matching with another sensor node. So even if one of the individual keys out of three keys is same between two or more sensor node due to the same x' or y' information still the pairwise key will be different as it is generated using all the three keys in the key ring set.

Since key generation is hash chain based, head node has the ability to generate individual keys for any node in its cluster as it knows the location of all the nodes in its cluster. The head node uses this concept later in the pair wise key generation mechanism. No sensor node of the cluster can generate individual keys of any other sensor node because they do not have the location information of any other node. Hash chains are lightweight cryptographic elements and are suitable for applications in WSN and they have the following properties:

- For a given cryptographic hash function h and an input string S, it is easy to calculate $h(S)$ but not possible to retrieve S from $h(S)$. Since cryptographic hash functions are one-way, it is also not possible to compute h^{-1} where $h(h^{-1}(S))= h(S)$.
- The hash function h has collision resistant property which means it is not possible to find two strings S and S' such that $h(S) = h(S')$.

4.2.2 Authentication of Sensor Nodes and Secure Pairwise Key Generation

We consider two sensor nodes *A* and *B* with identities ID_A and ID_B respectively in the same cluster and show how pairwise keys for them are generated (Figure 6).

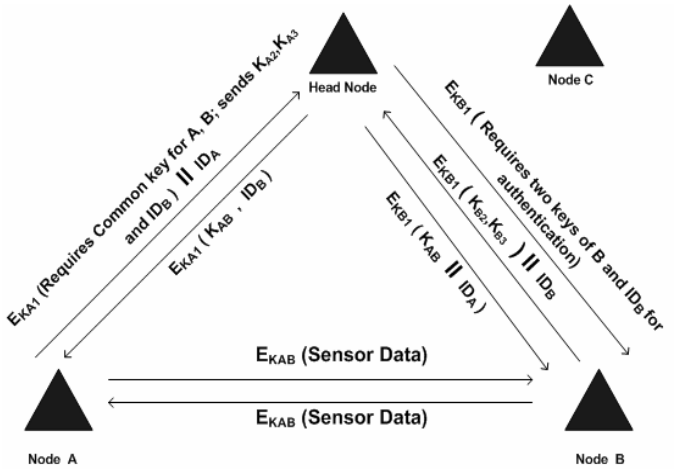

Figure 6. LH Scheme

Suppose *A* has K_{A1}, K_{A2} and K_{A3} and B has K_{B1}, K_{B2} and K_{B3}. These individual keys have been generated by the three hash chains discussed above. If node *A* wants to communicate with node *B*, it will require a symmetric pair wise key. The pair wise key generation starts by *A* sending its ID_A and an encrypted message E_{KA1} to *H*. E_{KA1} contains 3 entities: (a) two of the three individual keys of *A* chosen randomly and (b) the identifier ID_B of *B*. E_{KA1} is a message encrypted using the individual key of *A* (e.g., K_{A1}) and hence this key, $K_{A1,}$ is not included in the message. *A* sends this encrypted message E_{KA1} to *H* requesting a common pairwise key, K_{AB}, for communication.

The head node *H* checks the authenticity of these two nodes before it generates the pairwise key for *A* and *B*. *H* checks the identifier of *A* and initially assumes that *A* is a local node of the cluster. Since all the keys of *A* were earlier generated by using a hash

chain starting from H, it can re-hash multiple times and calculate all the three keys of A. It decrypts E_{KA1} (by applying the three keys of A using trial and error method) and get two keys of A in the message. The head node authenticates A if two of the three generated keys match with the key pair in the message. H also knows that A wants to communicate with B (the encrypted message sent by A to the head node includes the identifier of the node it wants to communicate with) so it generates the individual keys of B using hash chain and stores it into its memory together with the individual keys of A. H authenticates node B next. It sends an encrypted message E_{KB1} to node B requesting its ID information and the other two keys of node B. Node B decrypt this message E_{KB1}(by applying its three keys one by one using trial and error method). Node B sends back E_{KB1} (encrypted message containing ID_B and two other keys of B, say K_{B2} and K_{B3}). After receiving this information from node B, H decrypts the message and matches this information with the previously stored information of node B (ID_B) and the keys K_{B2} and K_{B3}. The authentication of node B ends successfully if the information matches. In the event of information mismatch, H may declare B as malicious and quarantine it from the rest of the cluster.

After a successful authentication of nodes A and B the common pairwise key generation starts. H randomly selects the individual keys of A and B (say K_{A1} K_{A2} K_{B2} K_{B3}) and generate $K_{AB} = K_{A1} \oplus K_{A2} \oplus K_{B2} \oplus K_{B3}$ (Common key for A & B generated by XORing). H sends K_{AB} and ID_B to node A by encrypting it with K_{A1} and K_{AB} and ID_A to node B by encrypting it with K_{B1}. Nodes A and B will decrypt this common pairwise key and ID information by using their respective keys K_{A1} and K_{B1}. Node A understands that this pairwise key is to communicate with a node in its cluster with identifier ID_B.

Similarly, node B understands that this pairwise key is to communicate with a node in its cluster with identifier ID_A. The algorithm for pair wise key generation is summarized below:

a. Node A sends its ID_A and an encrypted message E_{KA1} (containing two randomly chosen keys of A and ID_B) to H requesting a pairwise key $K_{AB.}$ The message is encrypted using one of the keys of A, say K_{A1}.
b. H decrypts the message using key K_{A1} (it can generate all the three keys of A using hash chain) and verifies node A is an authenticate node. It also generates the three individual keys of B.
c. H sends an encrypted message E_{KB1} to node B requesting its ID information and the other two keys of node B.
d. B decrypts this message E_{KB1} using K_{B1} and sends back an encrypted message E_{KB1} (containing ID_B and two other keys of B say K_{B2} and K_{B3}). The message is encrypted using one of the keys of B, say K_{B1}.
e. H decrypts this message using key K_{B1} and authenticates B.
f. H generates common pairwise key K_{AB} by XORing the randomly chosen keys of A and B. ($K_{AB} = K_{A1} \oplus K_{A2} \oplus K_{B2} \oplus K_{B3}$).
g. H sends the common pairwise key K_{AB} and ID_B to node A by encrypting it with K_{A1}.
h. H sends the common pairwise key K_{AB} and ID_A to node B by encrypting it with K_{B1}.

Node A and B decrypt the messages sent by H using their keys K_{A1} and K_{B1} respectively to recover K_{AB}. Node A and B may now communicate with each other using the common symmetric key.

In our scheme we have considered a scenario where two sensor nodes require common pairwise key from H before they can communicate. H authenticates these nodes before sending the common pair wise keys. In some scenarios a sensor node may try to communicate with many other sensor nodes, as a result, H may end up authenticating the sender node as many number of time as the number of nodes it want to communicate (multiple authentication) within a very short interval. This will incur significant processing cost which will vary with the size of the network and traffic leading to significant communication delay. We are actively investigating this issue we will report our remedy in our future work.

4.3 Location-Based Non Hash (LNH) Chain Scheme:

In our previous scheme (LH), the key generation and distribution is somewhat centralized. The individual key generation and later distribution of pairwise key is initiated by H inside the cluster. After the pair wise key has been generated H does not play any significant role. In our second scheme (LNH), the common pair wise key is generated by individual sensor nodes with some assistant from H. Thus, the pair wise key generation in this scheme is distributed. Unlike LH scheme here H does not generate pair wise key but acts as a third party in key generation. The dependency of H in common pair wise key generation in LNH scheme is less than that of LH scheme. Use of both schemes can vary depending upon the cluster size. Implementing hash chain based LH scheme for huge clusters can be sometimes tedious but it is more secure compared to LNH scheme

which can work well if the cluster size is bigger as it is simpler to implement. Figure 7 shows the operations of our LNH scheme.

4.3.1 Sensor Node Deployment and Secure Key Generation

In this scheme every node inside a cluster has a unique key which is stored in them prior to deployment. During deployment, the location information, sensor Id, and the unique individual keys of every sensor nodes are stored into *H* in a secure manner.

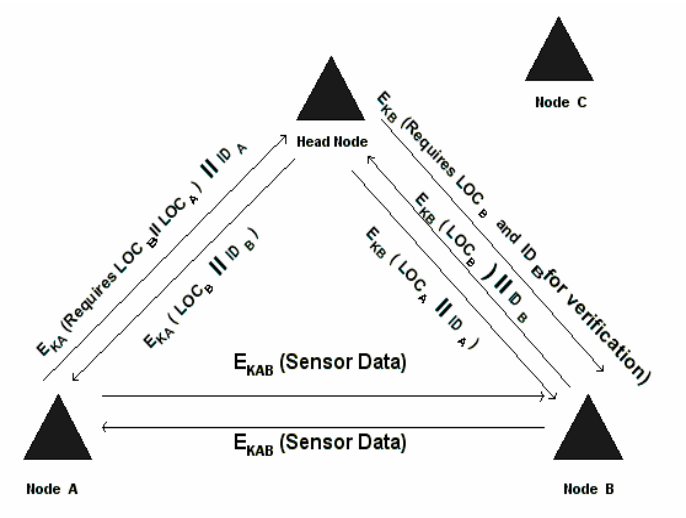

Figure 7. LNH Scheme

Similar to the LH scheme, we use location information of two sensor nodes wishing to communicate as a parameter to generate common pairwise keys. Two nodes (say A and B) wishing to communicate will require a common pairwise key, K_{AB}. The individual keys of these sensor nodes are K_A and K_B. Node *A* will send its sensor ID and an encrypted message E_{KA} to *H*. This message contains a request for the location information of node *B*. *H* receives the request and sends an encrypted message E_{KB} (containing ID_A) to *B* requesting its location information.

This message is an indication that Node A intends to communicate with B and hence B needs to send its location information to H. Node B will send its sensor ID and an encrypted message E_{KB} to H requesting node A's location information. H will identify node A and B by their IDs and can decrypt messages sent by them. As H has all the location information of the sensor nodes in its cluster, it sends the location information of node B to node A and vice versa by encrypting it with their individual keys. On receiving the location information from H, A and B will generate the common pairwise key K_{AB} ($Lat_A \oplus Lon_A \oplus Lat_B \oplus Lon_B$) by XORing location information. Unlike the previous scheme, the head node does not generate the pair wise key. It only acts as a third party in key generation.

All the communications done in this scheme are in encrypted form and hence cannot be eavesdropped. The scheme also does not require storing huge key sets in a sensor node. The mechanism is although lightweight but quite secured. The algorithm for pair wise key generation is summarized below:

a. Node A sends its ID_A and an encrypted message E_{KA} (requesting the location information of node B) to Head node H. The message is encrypted using the key of A, say K_A.
b. H receives the request and sends an encrypted message E_{KB} (containing ID_A) to B requesting its location information. This message is an indication that A intends to communicate with B and hence B needs to send its location information to H.
c. Node B sends its ID_B and an encrypted message E_{KB} (requesting the location information of node A) to H. The message is encrypted using the key of B, say K_B.
d. Node H decrypts the messages from A and B using key K_A and K_B.

e. Node H sends an encrypted message E_{KA} to node A containing node B's location information and an encrypted message E_{KB} to node B containing node A's location information.

f. Node A and B decrypt these messages and generate the common pairwise key K_{AB} by XORing of location information. ($K_{AB} = Lat_A \oplus Lon_A \oplus Lat_B \oplus Lon_B$)

Node A and B may now begin communication using this common pairwise key K_{AB}.

4.4 Strengths of Our Schemes as Compared to Other Existing Schemes

Unlike some other schemes developed earlier, our LH and LNH schemes are although lightweight but very effective as discussed below:

- Unlike most other schemes, ours do not require broadcasting of a subset of keys.
- Our schemes do not require storing large amount of information (for example, a subset of keys) inside a sensor node (except the head node) to compose a common pair wise key. This saves significant number of transmissions between nodes and storage space.
- No major calculations other than hash chain generation (which are lightweight cryptographic functions) are needed to generate pair wise keys.
- In our schemes we have used location information of sensor nodes for key generation. Location information is a metric unique to each sensor node. No two sensor nodes can have the same location. Also, it is not possible to find the location of a sensor node using the location of another sensor node. This means even if one node is compromised, the other nodes remain safe.

- Our schemes have a mechanism for authenticating sensor nodes before common pair wise keys between two sensor nodes can be generated. In this way, malicious sensor nodes can be identified easily within the cluster and *H* can take appropriate action.
- Our schemes perform well irrespective of cluster size. This is because there is less communications among nodes which is less susceptible to eavesdropping.
- Our schemes are robust and in the event of an eavesdropping, the encrypted messages cannot be decrypted as the intruder will not have the individual keys of a node. We assume that head nodes in our network are tamper resistant devices and cannot be compromised. Even if the intruder compromises other sensor nodes, it will not be able to generate individual keys of those nodes (since they are created using one way hash chains starting from the head node).
- The proposed schemes always guarantees that no matter how many regular sensor devices are compromised, the other non compromised devices can still communicate with 100% secrecy. The proposed schemes are always unconditionally secure against node capture attacks.

CHAPTER 5

PERFORMANCE ANALYSIS

We evaluated LH and LNH schemes with the EG scheme, Q-Composite scheme, Random Pairwise scheme, AP scheme, ECPKS scheme, USKS scheme, CPPS and CPKS scheme. As discussed above that key-distribution in broadcast based schemes are vulnerable and it is costly to maintain security. The above mentioned schemes broadcast their key or polynomial sets for pairwise key generation. Broadcasting keys is more costly in terms of processing power and battery life as a large portion of power is used in data transmission.

To avoid an increase in computational, power consumption and storage cost, unlike other schemes our schemes (LH and LNH) avoids key broadcast during common pairwise key generation process and therefore we expect our schemes to be more energy efficient as shown below. In our experiment we compared the total data transmitted in all the above schemes and total storage required in a sensor node during the pair wise key generation process. The schemes are evaluated assuming networks of all sizes. We initially assumed a network of 100 nodes in a cluster and increase the size by 100 nodes. The size of a key is assumed to be 128 bits. Interference is common in 2.4 GHz band. IEEE 802.15.4 applications (sensor nodes) have low quality of service requirements and may need to perform multiple retries for packet transmissions. This is especially true for data broadcast of key rings in a sensor network which may significantly affect the transmission cost between sensor nodes. To avoid complicated scenarios of significant

rebroadcast of keys in a sensor network due to loss of data, we assumed that all schemes are able to broadcast their keys with minimum retransmissions.

5.1 Power Consumption Analysis

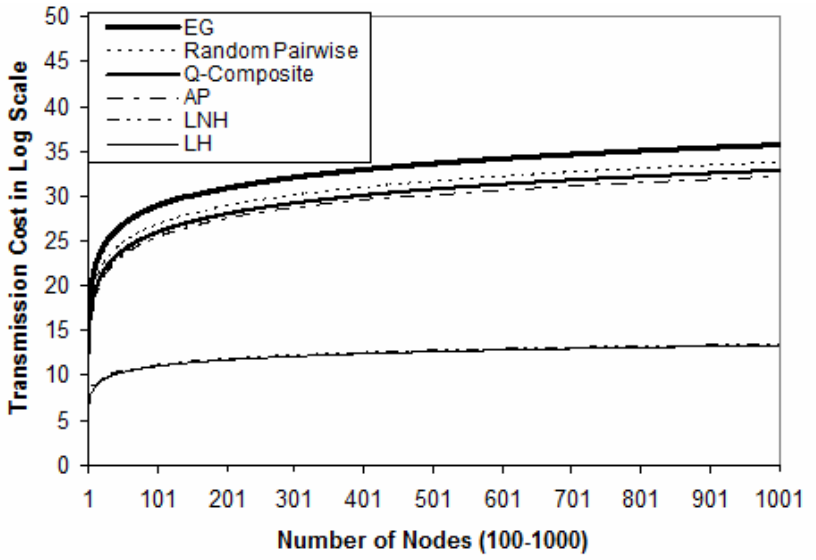

Figure 8. Comparison of Data Transmission in EG, Random pairwise, Q-Composite, AP with LH and LNH

Figure 8 and 9 show the result of our simulation comparing transmission cost between various other schemes. X axis denotes number of nodes. In Figure 8, for the sake of clarity and due to large values of y, we show the transmission cost in kilobytes using logarithm scale. Here Figure 8 shows that transmission cost of EG scheme is significantly higher than Q-composite and Random pairwise scheme. AP scheme works better than the above mentioned scheme even with increased number of nodes. Due to unicast transmissions for pairwise key generation, both of our schemes (LH and LNH) have relatively lower cost as compared to other schemes.

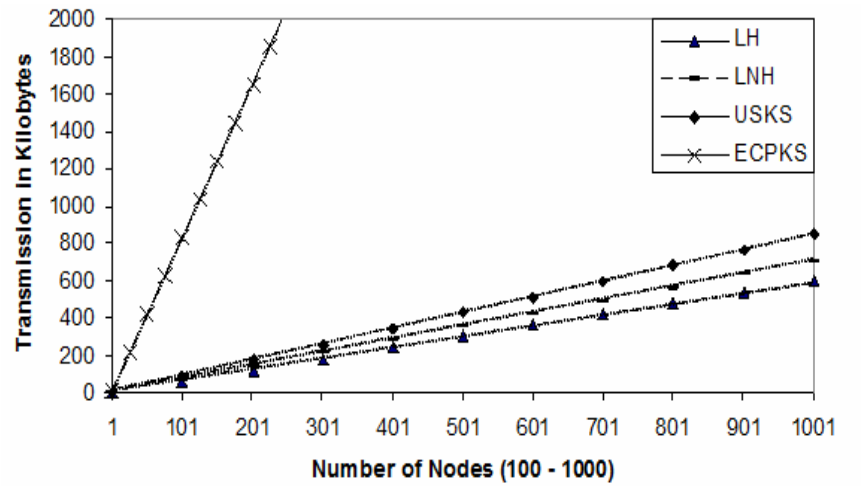

Figure 9. Comparison of Data Transmission in ECPKS, USKS with LH and LNH

Figure 9 shows the comparison of LH and LNH schemes with ECPKS and USKS schemes. ECPKS scheme stores higher number of keys inside sensor memory during key prioritization phase. After key prioritization only highest priority keys are kept and rest is discarded. In comparison to USKS scheme it uses more message communication and therefore is costly as shown in Figure 9. On the other hand LH and LNH scheme use less message transmission to find the common pairwise key and perform slightly better than USKS scheme but much better in comparison to ECPKS scheme.

Both LH and LNH schemes perform similarly during the data transmission experiment.

5.2 Data Storage Analysis

Figure 10 and 11 shows the cost of storage of key ring sets in the memory. Since key ring sets are used to generate pairwise keys, they are kept in the program + data memory of the node. For values of N = 4900-5000, key ring set storage requirements for EG scheme is more than 128 kilobytes, thus making it completely insignificant in terms of usage for most of the contemporary sensor nodes, including the popular Mica series,

IMotes and Telos sensors (except high end sensors like Sun SPOTS [28, 29], which has 512 kilobytes of RAM). Q-Composite scheme performs better than Random pairwise scheme for large values of N. It still takes more memory as compared to our LH scheme (14 kilobytes in Q-Composite as compared to approximately 2.5 kilobytes in our LH scheme for N=10000). During deployment of sensors in LNH scheme, the location information, sensor id information and the unique individual keys of every sensor nodes are stored into the head node in a secure manner. This causes the scheme to perform worse than the LH and Random pairwise scheme but better than Q-Composite and EG scheme. The LH scheme performs best in terms of data transmission.

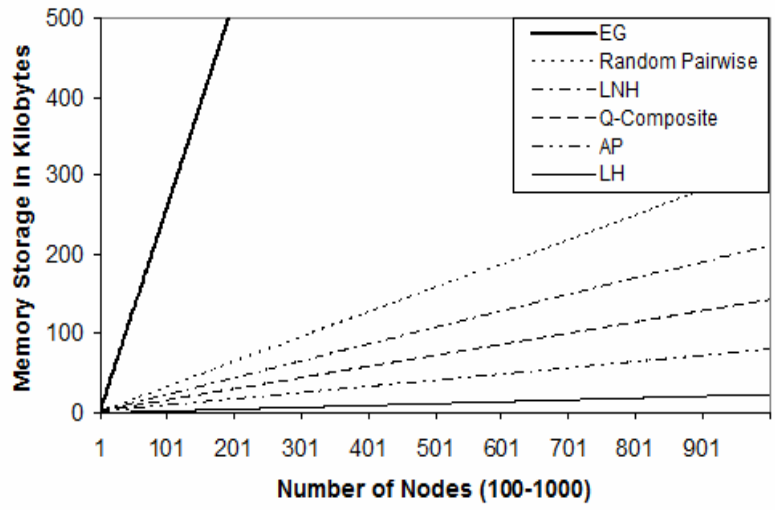

Figure 10. Memory Storage comparison of EG, Random pairwise, Q-Composite, AP with LH and LNH schemes

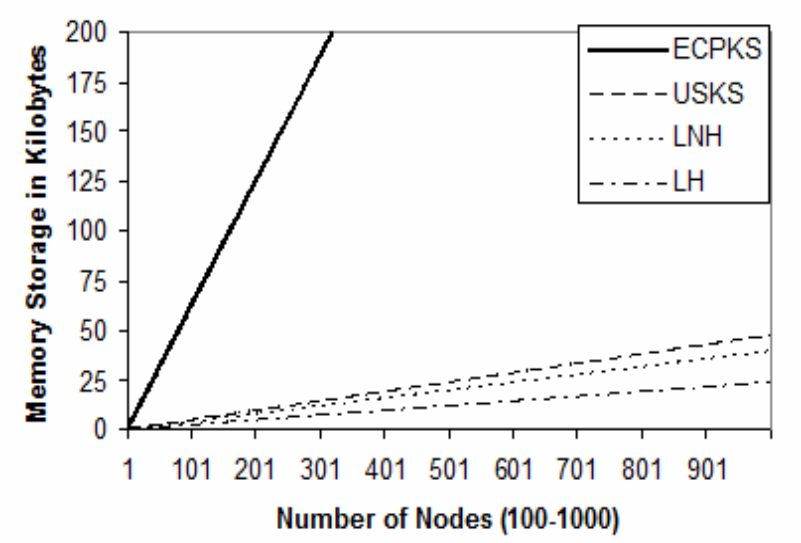

Figure 11**.** Memory Storage comparison of ECPKS, USKS, LH and LNH schemes.

In Figure 11 we have shown the memory storage comparison between ECPKS, USKS, LH and LNH schemes. During deployment the set up server selects a set S_1 of n sensor nodes whose expected locations are closest to any node a. Now if all the nodes want to communicate between themselves they are required to have a common pairwise key between themselves. So for each node b in S_1 set up server stores n key-plus-id combination (k_{ab}, id_a) into b's key ring and also n key-plus-id combination (k_{ab}, id_b) into a's key ring. This type of setup leaves very small memory left to be used as application in sensor devices such as smart dust sensor which has only 8 K bytes of program memory and 512 bytes of data memory. Also in USKS scheme before deployment the set up server stores id_s, master keys, n key plus id combination $K_{Hi,\ uj}$, id_{uj} (key and id combination of H and L sensors respectively) and the polynomial share of all H sensor to each H sensor. Also each L sensor are loaded with its own id, master key and l key plus id combination $K_{u,\ vj} = \text{PRF}_{MKvj(idu)}$ where u and v are L sensors, MK_{vj} is the master key of any sensor v_j and id_u is the id of sensor u. Though USKS works better than ECPKS but

our schemes LH and LNH performs best in terms of memory storage as shown in Figure 11.

5.3 Security Analysis

In this section we compare security against sensor node capture of our schemes with that for the existing schemes.

We compare our scheme LH and LNH with EG scheme, Q-Composite Scheme, Random Pairwise Scheme, AP scheme, ECPKS scheme, CPPS and CPKS scheme. Here we consider a scenario where 100 regular sensor nodes have been captured in a network and we keep on increasing the size of the network by 100 more captured nodes. The resilience against node capture attack of a key establishment scheme is measured by estimating the fraction of total secure communications that are compromised by a capture of c nodes not including the communication in which the compromised nodes are directly involved. For example, for any two non-compromised sensor nodes *a* and *b*, we have to find out what is the probability that the adversary can decrypt the secret communications between *a* and *b* when *c* sensor nodes are already compromised. If Pe(c) denotes the fraction of total secure communications compromised after capturing c sensor nodes by an attacker in a sensor network and if Pe(c) = 0, we call a key establishment scheme as unconditionally secure against node capture or perfectly resilient against node capture. We can see from the figure 12 that even with a small number of *c* captured nodes, EG scheme reveal a large fraction of total secure communications between non-compromised sensor nodes in the network.

The security of CPPS scheme shows that it performs well as long as number of captured nodes is small but as more number of nodes is captured CPPS scheme works

less better. ECPKS scheme performs better than CPPS scheme in terms of certain fraction of revelation of secure communication links between non compromised nodes. Only CPKS, LH and LNH provide unconditional security against regular node capture attacks. We have assumed *H* nodes (cluster head) are equipped with tamper-resistant technology [36]. For a network of 1000 nodes we need only 10 tamper resistant *H* nodes assuming we have 100 nodes in a cluster. It is reasonable to assume that powerful *H* nodes are equipped with this technology.

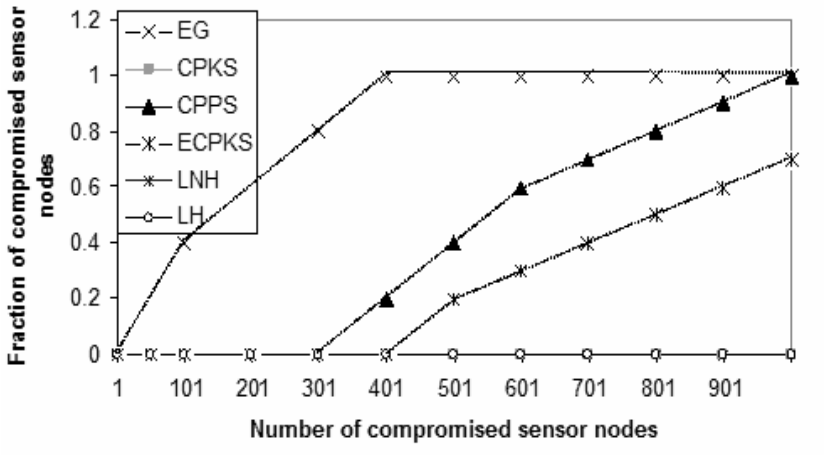

Figure 12. Security Analysis of EG, CPKS, CPPS, ECPKS with LH and LNH schemes.

However for *H* nodes to be not tamper resident the attacker can get valuable sensor node information such as hashing function, location information etc. Therefore it can generate individual sensor keys inside a single cluster and can compromise the communication between two regular sensors by XORing the various possible combinations of individual sensor keys. Our future work will be in this area of providing unconditionally security to *H* nodes. However we have a better tradeoff between security

vs. transmission and storage cost of our schemes with all other current schemes. We outperform most other schemes in this area.

CHAPTER 6

CONCLUSION

In this work we have developed a unicast based pairwise key generation and distribution scheme. A prominent feature in the key generation process includes generation of one way hash key chains and use of location information which adds to the security of our scheme. Broadcast and storage of key ring sets have been avoided (due to the inherent feature of unreliability of data broadcast in sensor nodes) unlike other schemes. This idea has led to significant reduction of cost in terms of transmission and storage.

We have used location information of sensor nodes for key generation which is a metric unique to each sensor node. The scheme performs well irrespective of network size because there is less communications among nodes which is less susceptible to eavesdropping. Our scheme is robust and in the event of an eavesdropping, the encrypted messages cannot be decrypted. Right now we assume that head nodes in our network are tamper resistant devices and cannot be compromised. In future we intend to develop a prototype for health care management that will address secure communication of medical data between medical sensors and handheld device of mobile patient called personal wireless hub (PWH) inside a wireless body sensor network (WBSN) using unicast based LH and LNH schemes.

BIBLIOGRAPHY

1. Bharathidasan A. and Ponduru V. Sensor Networks: An Overview. In *Proceedings of IEEE Infocom*, Hongkong, 7-11 March 2004.
2. Akyildiz I.F., Su W., Sankarasubramaniam Y., and Cayirci E. A Survey on Sensor Networks. In *Proceedings of* IEEE *Communications Magazine*, vol. 40, no.8, pages 102-114, August 2002.
3. Perrig A., Stankovic J., and Wagner D. Security in Wireless Sensor Networks. In *Proceedings of Communications of the ACM*, 47(6), 54-57, June 2004.
4. Haowen C., and Perrig A. Security and Privacy in Sensor Networks. In *Proceedings of IEEE Computer Society*, vol. 36(10), October 2003.
5. Perrig A., Szewczyk R., Wen V., Culler D. and Tygar J.D. SPINS: Security Protocols for Sensor Networks. In *Proceedings of* IEEE *Infocom*, Anchorage (Alaska), 22-26 April 2001.
6. Spinellis, D. and Katsikas, S. 1999. Trusted Third Party services for deploying secure telemedical applications over the WWW ‖ . *Computers and Security*, vol. 18, No. 7, 1999.
7. Interactware (2009), *Mobile Health Monitoring*, available at http://interactware.com/2010/08/18/white-paper-on-mobile-health-monitoring/ [accessed on August 1, 2010].
8. Accu-Chek (2008) *Blood Glucose Monitoring Systems*, available at https://www.accu-chek.com/index.html [accessed on 8 June, 2010].

9. CHCF (2010), *Health Care Costs 101*, available at http://www.chcf.org/publications/2010/04/health-care-costs-101 [accessed on 13 June, 2010].
10. Robert Wood Johnson Foundation (2010*), Chronic Care: making the case for On-going Care*, available at www.rwjf.org/files/research/50968chronic.care.chartbook.pdf [accessed on 13 June, 2010].
11. Wu, S.Y. and Green, A. (2000) '*Projection of chronic illness prevalence and cost inflation*' Santa Monica, CA, RAND Corporation.
12. CDC (2009), *Ambulatory Care use and Physician visits*, available at http://www.cdc.gov/nchs/fastats/docvisit.htm [accessed on June 13, 2010].
13. Glied, S. A., Prabhu, A. and Edelman, N.H., (2008) 'The Cost of Primary Care Doctors', *NBER Working Paper No. 14568*.
14. HHS (2002), *Projected Supply, Demand, and Shortages of Registered Nurses: 2000-2020*, available at http://www.ahcancal.org/research_data/staffing/Documents/Registered_Nurse_Supply_Demand [accessed on June 15, 2010]
15. Camtepe S. A. and Yener B. Key Distribution Mechanisms for Wireless Sensor Networks: A Survey. In *Proceedings of Technical Report TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department*, March 2005.
16. Eschenauer L. and Gligor V.D. A Key-Management Scheme for Distributed Sensor Networks. In *9th ACM Conference on Computer and Communications Security*, Washington DC, pages 41-47, 18-22 November 2002.

17. Chan H., Perrig A., and Song D. Random Key Predistribution Schemes for Sensor Networks. In *Proceedings of IEEE Symposium on Research in Security and Privacy*, California, pages 197-213, 11-14 May 2003.

18. Jin, G. and Park, M. 2006. An Indoor Localization Mechanism Using Active RFID Tag. *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing* - Volume 1, pages 40-43 June 2006.

19. Liu D. and Ning P. Establishing Pairwise Keys in Distributed Sensor Networks. In *Proceedings of 10th ACM Conference on Computer and Communications Security CCS*, Washington DC, v.35 n.10, pages 54-62, 27-30 October 2003.

20. Zhu S., Setia S., and Jajodia S. Leap: Efficient security mechanisms for large-scale distributed sensor networks. In *Proceedings of 10th ACM Conference on Computer and Communications Security (CCS),* Washington DC, pages 62–72, 27-30 October 2003.

21. Perrig A., Canetti R., Song D., and Tygar D. Efficient authentication and signing of multicast streams over lossy channels. In *Proceedings of the IEEE Symposium on Security*, May 2000.

22. Goldreich O., Goldwasser S., and Micali S. How to construct random functions. *Journal of the ACM 33*, 4 (October), 792–807.

23. Liu D. and Ning P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In *Proceedings of 10th Annual Network and Distributed System Security Symposium*, pages 263- 276, February 2003.

24. Liu D. and Ning P. Multi-level mTESLA: Broadcast authentication for distributed sensor networks. In *Proceedings of ACM Transactions in Embedded Computing Systems (TECS)*, Vol. 3, No. 4, pages 800-836, November 2004.

25. Aakvaag N., Mathiesen M. and Thonet G. Timing and Power Issues in Wireless Sensor Networks: An Industrial Test Case. In *Proceedings of 2005 International Conference on Parallel Processing Workshops*, pages 419-426, 2005.

26. Zhang Y., Liu W., Lou W. and Fang Y. Securing sensor networks with location-based keys. In *Proceedings of Wireless Communications and Networking Conference, 2005 IEEE* Volume 4, Issue, 13-17 March 2005 Page(s): 1909 - 1914 Vol. 4.

27. Huang D., Mehta M., Medhi D. and Harn L. Location-aware key management scheme for wireless sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*, pages 29 – 42, October 2004

28. http://www.sunspotworld.com.

29. www.sunspotworld.com/docs/Purple/SunSPOT-OwnersManual.pdf.

30. Das A. K. An unconditionally secure key management scheme for large-scale heterogeneous wireless sensor networks. In *First IEEE International Conference on Communication Systems and Networks (COMSNETS 2009),* pages 1–10, 2009.

31. Du X., Xiao Y., Guizani M. and Chen H.-H. Chen. An effective key management scheme for heterogeneous sensor networks. Ad Hoc Networks (*Elsevier*), 5(1):24–34, 2007.

32. Das A. K and Sengupta I. A key establishment scheme for large-scale mobile wireless sensor networks. In *4th International Conference on Distributed*

Computing and Internet Technology (ICDCIT 2007), LNCS 4882, pages 79–88, 2007.

33. Liu D. and Ning P. Improving key pre-distribution with deployment knowledge in static sensor networks. *ACM Transactions on Sensor Networks*, 1(2):204–239, 2005.
34. Das A. K. ECPKS: An Improved Location-Aware Key Management Scheme in Static Sensor Networks. *International Journal of Network Security (IJNS)*, 7(3):358–369, 2008.
35. Blundo C., Santis A. D, Herzberg A, Kutten S, Vaccaro U, and Yung M. "Perfectly-secure key distribution for dynamic conferences;' in Advances in Cryptology- *CRYPTO '92*, LNCS 740, Berlin, August 1993, pages 471-486
36. ThomasNet "http://news.thomasnet.com/fullstory/Safety-Sensor-has-tamper-resistant-design-6653".

VITA

Debargh Acharya was born on January 19th, 1983 in India. He spent most of his childhood and teenage years in Lucknow, one of the cultural capitals in India and South East Asia. He completed his Bachelors in Computer Science from Uttar Pradesh Technical University (UPTU), India. After graduating in June 2006 he worked as an instructor in Sri Ram Swaroop College of Engg. And Management, affiliated to UPTU, India for 1 year. In the fall of 2007 he moved to the United States for his Masters in Computer Science at the University of Missouri Kansas City and started to work under Dr. Vijay Kumar in the field of Security in Wireless Sensor Networks and Pervasive Health Care. He has authored and published 3 peer-reviewed conference papers and submitted one journal paper. His research interests include Wireless Sensor Networks, Security in Pervasive Healthcare and Algorithm design. He started working at Commerce Bankshares as a Security Analyst intern in the summer of 2010. Later he joined the Business Development Team at Commerce Bankshares as an IT Developer where he is presently working now.

Publications

1. Debargh Acharya, Vijay Kumar and Debopam Acharya; **DVD: A Secure Unicast based Pairwise Key Generation Scheme for Wireless Sensor Networks**, **IEEE SENSORCOMM 08**, August 25-31, 2008 - Cap Esterel, France.

2. Debargh Acharya; **Security in Pervasive Health Care Networks: Current R&D and Future Challenges, mdm, pages305-306, Eleventh International Conference on Mobile Data Management, 2010,** Kansas City, USA.

3. Debargh Acharya and Vijay Kumar, "**A Secure Pervasive Health Care System Using Location Dependent Unicast Key Generation Scheme**," **19th ACM International Conference on Information & Knowledge Management, PIKM Workshop 2010**, Toronto, Canada.

4. Debargh Acharya and Vijay Kumar, "**Security in Wireless Sensor Networks Based on Location Technologies: LH and LNH, " International Journal of Sensor Networks, 2010** (under review).