

**A Hybrid Approach to Authenticated Key Agreement with
Rekeying for Secured Body Sensor Networks**



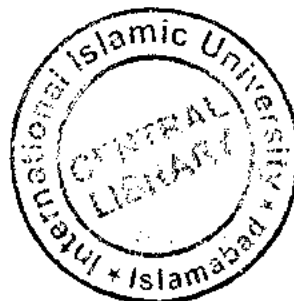
Muhammad Asad
450-FBAS/MSCS/F08

Supervised by
Professor Dr. Muhammad Sher



Department of Computer Science and Software Engineering
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad

2014



Accession No. TH 13555 k

MS
004.19
MUH

size 30000
OC 2
small 204.

DATA ENTERED

Hybrid computers

Analog computers

A Hybrid Approach to Authenticated Key Agreement with Rekeying for Secured Body Sensor Networks



Muhammad Asad
450-FBAS/MSCS/F08

A Thesis submitted to I.I.U. in partial fulfillment of the requirement for the Degree of MSCS

Supervised by
Professor Dr. Muhammad Sher

Department of Computer Science and Software Engineering

Faculty of Basic & Applied Sciences

International Islamic University, Islamabad

2014

ii

Department of Computer Science & Software Engineering,
International Islamic University Islamabad

Date:

Approval Certificate

It is certified that we have read the thesis titled "*A Hybrid Approach to Authenticated Key Agreement with Rekeying for Secured Body Sensor Networks*" submitted by *Muhammad Asad* Reg. No. 450-FBAS/MSCS/F08. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the degree of **Master of Science in Computer Science**.

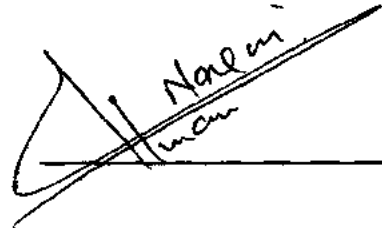
1. External Examiner

Dr. Muazzam Ali Khan Khattak
Assistant Professor, NUST
School of Electrical Engineering & Computer Science




2. Internal Examiner

Dr. Syed Husnain Naqvi
Assistant Professor, FBAS
International Islamic University,
Islamabad



3. Supervisor

Professor Dr. Muhammad Sher
Dean, Faculty of Basic and Applied Sciences
International Islamic University,
Islamabad


21.5.14

Dedicated to
My Beloved
Parents

DECLARATION

I hereby declare and affirm that this thesis neither as whole nor as a part there of has been copied out from any source. It is further declare that I have completed this thesis on the basis of my personal efforts, made under the science guidance of my supervisors. If any part of thesis report as proven to be copied out or found to be reproduction of some other I shall stand by the consequences. No portion of the work presented in this report has been submitted in support of an application for other degree or qualification of this or any other university of learning.

**Muhammad Asad
450-FBAS/MSCS/F08**

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious and the Most Merciful All praise and glory to Almighty Allah (Subhanahu Wa Ta'ala) who gave me the courage and patience to carry out this work. Peace and blessings of Allah be upon His last Prophet Muhammad (peace be upon him), said: "Allah makes the way to Jannah easy for him who treads the path in search of knowledge." First and foremost, I would like to thank my supervisor **Professor Dr. Muhammad Sher** for accepting, supporting and allowing me to take the liberty to follow my research interests as well as for continuous guidance, valuable advice, immense effort, and thoughtful discussions throughout my research. I would like to thank my Family, specially my father for all their love, understanding, prayers and financial support. Their prayers and encouragement always help me to take the right steps in life. I would like to give special thanks to all my colleagues and friends. I thank **Mr.Nizamuddin** for exchanging ideas, motivation social and moral support throughout my work.

Muhammad Asad

Abstract

In medical system tiny devices or sensors used in, on, near or as required to human body in such a way that they gather data, process data, make communication with each other. These tiny devices when especially used for human body then formally called Body Sensor Network (BSN). The security measures, methods and implemented formwork for WSN are not optimal for BSNs, because of distinct features of BSN. The heart of secure communication is key management protocols. Key managements provide and manage the cryptographic keys to facilitate fundamental security features such as confidentiality, authentication and integrity. Achieving key agreement in BSNs is a complex task. Many key agreement schemes for BSN have deficient in sensor addition, revocation, and rekeying properties, which are very important. Our proposed hybrid approach cope these shortcomings by providing node rekeying properties, node addition, revocation as well as to overcome the high cost of asymmetric cryptography session key exchange. Our hybrid proposed key agreement model is based on (ECC) Elliptic curve cryptography and symmetric cryptography. Our proposed scheme does not dependence upon individual sensors and it trusts upon the base station. Instead of loading bulk of keys into each node, after installation our protocol establishes session keys between nodes according to a specific routing algorithm. In this scenario, each node doesn't have to share a key with all of its neighbors, only those concerned in the routing path; this plays a key role in increasing the resiliency against node capture attacks, the network storage efficiency, communication overhead and computation cost. The proposed scheme reduced normally 74% memory requirements for keys storage, 80% computation cost and 60% communications overhead and also provides rekeying features. Finally we assessed our scheme from the BSN security viewpoint and evaluate its performance in comparison with other schemes.

Acronyms

AES	Advance Encryption Standard
BSN	Body Sensor Network
RSA	Rivest Shamer Adlman
DES	Data Encryption Standard
WSN	Wireless Sensor Network
ECC	Elliptic Curve Cryptosystem
DHECC	Diffe Helman Elliptic Curve Cryptosystem
PKC	Public Key Cryptography
SKC	Symmetric Key Cryptography
BS	Bio-Sensor
MBS	Medical Bio Sensors
WBAN	Wireless Body Area Network
BAN	Body Area Network
BS	Base Station
GW	Gateway
MEMS	Micro Electro Mechanical Systems
DoS	Denial of Services
WN	Wireless Network
PKS	Public Key System
SKS	Symmetric Key System
PKs	Public Keys
SKs	Symmetric Keys
SSK	Secure Symmetric Key
GRKs	Generating Random Keys
MAC	Message Authentication Code
ECG	Electro-Cardio Graph
IPI	Inter Pulse Interval
RDP	Resurrecting Duckling Protocol
KDC	Key Distribution Centre
CH	Cluster Head
CN	Cluster Node
Enc	Encryption
Dcn	Decryption
PKE	Public Key Encryption
PKD	Public Key Decryption
MU	Medical Units
NIST	National Institute of Standards and Technology
ME	Modular Exponentiations
ECPM	Elliptic Curve Point Scalar Multiplication

Contents

Chapter 1	1
1. Introduction	2
1.1 Wireless Communication.....	2
1.2 Cram of WSN	2
1.3 Body Sensor Network	3
1.3.1 Extension of BSN.....	4
1.3.2 BSN Applications.....	4
1.4 Problem Recognition.....	5
1.5 Role of Contribution of Thesis	6
1.6 Thesis Organization.....	6
Chapter 2	7
2. Body Sensor Network	8
2.1 Architecture of BSN.....	8
2.2 Body Sensor Network's Requirements.....	10
2.3 Challenges for Body Sensor Network.....	10
2.3.1 Placement/ Implementation Challenges.....	12
2.3.2 Fidelity Challenges.....	12
2.3.2 Security Challenges.....	13
2.4 Key Concord in BSN	14
Chapter 3	15
3. Literature Survey.....	16
3.1 Different Publish Scheme's Review	16
3.2 Review Conclusion	20
Chapter 4	21
4. Problem Statement	22
4.1 Proposed Structure.....	23
4.2 Scope Of Intended Solution	23
4.3 Research Purpose.....	24
4.4 Role of Research	24
Chapter 5	25
5. Proposed Mechanism	26
5.1 Designed Marks	26
5.2 Proposed Scheme Structure.....	26
5.3 Terminologies	27
5.4 Proposed Methodology.....	28
5.4.1 Keys Pre-loading Phase.....	28
5.4.2 Session Keys Setup Phase.....	29
5.4.3 Re-keying Phase.....	30

Chapter 6	32
6. Implementation and Results Validation	33
6.1 Simulation.....	34
6.2 Result Validation	35
6.3 Cost Analysis.....	35
6.3.1 Communication Cost.....	35
6.3.2 Communication Overhead.....	36
6.3.3 Computation Cost and Key Computation Time Analysis.....	37
6.3.4 Memory Requirements Analysis.....	38
6.4 Security Analysis of Our Scheme.....	39
 Chapter 7.....	 41
7.1 Conclusion.....	42
7.2 Future Work	42
 References.....	 43

List of Table

Table 5.1 Planned Technique Notations.....	27
Table 5.2 Pre-loaded keys phase	28
Table 5.3: Key Establishment	29
Table 5.4 Re-keying phase	31
Table 6.1: Simulation Parameter for BSN *IEEE 802.15.6*	34
Table 6.2 Communication overhead Reduction for Sensor.....	36
Table. 6.3 Memory Requirements for Sensor.....	38

List of Figures

Figure 2.1 Body Sensor Network.....	09
Figure 3.1 Key management models of [15].....	19
Figure 5.1 Proposed Scheme Network Model.....	28
Figure 5.2 Session Key Establishment.....	29
Figure 5.3 Re-keying phase.....	31
Figure 6.1 Communication Energy Cost for Different Rounds.....	35
Figure 6.2 Communication overhead of key Management scheme.....	36
Figure 6.3 Computation cost of key Management scheme.....	37
Figure 6.4 Memory Requirements for Sensor.....	38

1

INTRODUCTION



1. Introduction

Modern technological developments enhance the whole world in all aspect of life living methods. Fast changing tends the world to a new way of observation to all area of life. Every days new inventions, research and necessities picked up the human thinking level so high that it should looked that without usage of technology no solution for each and every problem. Humans now introduced not only the war equipment to conquer other ideas but also take over each other in daily usage equipments of technology. Especially the medical area is most pruned era of know-how maturity.

1.1 Wireless Communication

From last few decades' Wireless communication is at on its peak. Wireless Communication tried to cover each growing area of life. It made simple and easy communication on the ground as compared to wired communication.

Wireless Communication gave significant enhance in hundredth area mainly, portable and wireless systems. Like these networks, Wireless Sensor Network (WSN) is major fast emergent network system that upshot countless era of daily know-how.

1.2 Cram of WSN

Trimness and petite equipment advancement pick up artful and expansion manufactory to produce alike devices that should be petite in magnitude, superior execution potential, adequate memory and framework. Development of sensors and petite devices make world into a new global aspect and domain. Grouping these devices into such a design of forming a network such that they can communicate with each other and can share data known as Wireless Sensor Network (WSN).

The preemptive WSN introduced many applications that are needed in daily life areas and monitoring of medical activity is one crucial area. WSN is of two types according to their hardware design working these are heterogeneous and homogenous. Moreover, WSN can be classified in hierarchical and scattered according to the network deployment role. The study about WSN opened much more research interest due to its widely and shortly coming devices in daily

life usage application. As WSN, information is transmitted over air so a strong security mechanism is required in order to meet secure communication.

1.3 Body Sensor Network

As like other areas, the medical area also needs small and low price devices that support to enhance the functionality of this area. In this area as patient is main object, therefore those types of sensors needed that can protect patient body from side effects. Unusual courtesy and visage are required due to distinct features and behaviors of human. Thus, trimness, thin, cost decline and able to hang or wear sensors necessitate in medical area. As these sensors set up on patient, hospital examine structure or in medical care parts they figure out Wireless Area Network (WAN) and especially on a human body affixation these tiny devices then called to be as Body Sensor Network (BSN).

Formally, BSN also called as Wireless Body Area Network (WBAN) either Body Area Network (BAN). In 1996 the T.G. Zimmerman introduced thought about wireless body area network (WBAN) [2]. Presently, healthcare appliances make use of wireless body sensor network that is one most remarkable practice of WSN technology. It is well known technology because it provides proper diagnosis and cure on the spot. In BSN sensors that are used for patient may place inside, outside, close to or as needful to human body in such a manner that they collect data, make possible operation on data, exchange information with each other and process signals if assimilation required and send information to the Base Station (BS). In hospital, little power petite sensor device is attached or tie up on the patient body like that it doesn't agitate typical daily basis works of human.

The body area network turf is an interdisciplinary region which could tolerate inexpensive and uninterrupted health monitoring with real-time updates of medical reports through the network. A number of intelligent physiological sensors can be integrated into a wearable wireless body area network, which can be used for computer-assisted rehabilitation or early detection of medical conditions. This area relies on the feasibility of implanting very small biosensors inside the human body that are comfortable and that don't impair normal activities. At this time, the level of information provided and energy resources capable of powering the sensors are limiting.

1.3.1 Extension of BSN

BSN made revolution changes in health care system. BSN animate the whole domain of medical system in such a way that surveillance and monitoring of patients is seems to be not too much dense and cumbersome as was in traditional systems. Development of BSN has given birth to health care units from last ten year and especially in 2-3 years. From few last year's BSN has emerged as one of the industry standard. "IEEE 802.15.6" group is defining consistency of the radio transition protocols for appliances in Body Area Network. Study of interests in BSN going to its peak meeting upon the requirement for the industry of 21st century. Main attempt of acute part of this exertion is as group effort, encouragement and knowledge sharing through researchers, design makers and health patrons on diverse BSN facilities. My study is also come what to do study research in this era, in particular to the key authentication as well as safety measures of BSN.

1.3.2 BSN Applications

BSN introduced many more application day by day. BSN sensors that are design especially for human body need special interest caused by compassion of human organization i.e. Heat, Blood Pressure. Development of "Smart Life Shirt" (2009) [6] put patients into a complete care unit without disturbing their daily life activities.

Taking to the real life examples the [33] Germantown, Maryland, USA – September 12, 2011 - Sensors for Medicine and Science, Inc. (SMSI) announced that first time an implanted biosensor used for diabetes's patient. The data showed high level of glucose accuracy, with 77.6% and 19.2% of the data in the A and B zones of the Clark Error Grid, respectively. The mean absolute relative difference was 12.2%. The results also support the sensor goal of achieving implant time greater than six months.

"We are pleased to report these findings as a first step to realizing a viable long-life implanted sensor to help millions of people with diabetes manage their glucose better," said Tim Goodnow,



Ph.D., CEO and President. "While still early, the pilot study showed comparable performance as current continuous glucose devices."

Moreover wearable sensors, implantable system and diagnostic sensors explored the utilitarianism of BSN technology in medical era. Like our aging people, mostly people suffer in very growing chronic medical conditions such as heart disease, diabetes, worsen surgery, fracture in main limb and stomach disease etc. These life sustaining chronic conditions require continuously and remotely monitoring. So BSN cover all such threatening situations by providing quick response to medical physicians as from near or at from distance. It is too much time saving response from both sides i.e. from patient reporting to medical professionals and from medical team to making decision upon report of patient. Another great contribution of BSN in health care system is that in emergency and disaster situation, this technology can be provided more quickly and urgently so that medical professional's made unbeatable solutions to effected area and their people.

- A BSN provides quick response upon threatening situations to medical physicians as from near or at from distance like heart attack and other vital signs.
- A BSN network performs automation process like a diabetic patient if insulin levels reduced then inject insulin through a pump.
- Such machinery also implies to test in different games for physical assessment.
- BSN also used in monitoring areas in particular as services inspection.

1.4 Problem Recognition

Against all these development that made revolutionary changes in health system, the heart of system is the communication platform. BSN uses wireless infrastructure that is very critical domain in mode of data transfer. So, it is very important issue to make data transfer infrastructure secure in BSN as compared to traditional wired system. BSN nodes communicate using air medium therefore protection and privacy of data transfer could not be compromised. Specially, in medical system it leads to false treatment if data is conciliation or links not secure between sensors. Lack of security measures not only breach the patient privacy but also potentially provide access to opponent to modify real data that results in wrong treatment and diagnosis. Therefore, security measures for BSN should be self-configurable, well defined and minimized. When

cryptography is used to meet the security requirements then most important role of cryptography in secure communication is key management protocols. The core duty of key management is make possible safe and secure links and paths between neighbor entities in network, make sure that data will exchange in multi-hop scenario. As a normal scenario we can say that key management is too much needed in security management according to data exchange scenarios. So, key management plays a vital role in cryptography schemes.

The traditional methods of key agreement have be deficient in; either security potential or of memory or computation cost. Using only symmetric key ideas, scalability and security harms arise. Beside this if only public key system pertain in that case computation cost and key storage memory related pros identifies. Our research work is based on a hybrid system in which both schemes involve. Our scheme will cope over energy issues, memory requirement and provides better security and scalability. Proposed scheme guaranteed about secure and genuine key agreement with rekeying for body sensor networks.

1.5 Role of Contribution About Thesis

This is a novel and innovative idea key agreement in BSN. The key purpose of research effort is to appraise and assess new security technique for proficient and protected communication in BSN to realize low computation cost, communication cost and memory storage.

1.6 Thesis Organization

Remaining study and idea is categorized as following.

1st and 2nd chapters describe the research topic theory relating to BSN, its purpose, capacity, design structure, security problems and the core one topic key management. Literature review is discussed in chapter 3, multiple previous schemes studied and markup their gratefulness and hindrances. Chapter 4 discussed problem manifesto and problem synopsis. Complete detail of proposed solution is written down in chapter 5. In Chapter 6 implemented experimental outcomes of proposed idea and at last chapters 7 we will discuss summary and prospective work of our study is mentioned.

2 BODY SENSOR NETWORK



2. Body Sensor Network

Health area is directed to focus on patient that is heart of this system needs such sensors structural design that good for human's tissues. Human body contains discrete characters, dominion and variable deeds so; deployment, expansion and designing of tiny devices like such eventual necessitate unique features as well as attentions. As a result wearable, miniatures, small fry and cost diminution devices entail in medical care system. When these devices deploy on a human body, hospital surveillance arrangement or in health facility department they constitute a environmental network formally called Body Sensor Network (BSN).

Mainly BSN covered twofold benefit for medical era. First is that ,it allow medical physicians to monitor patient at their home, therefore elderly or patient with chronic diseases get benefit of treatment and medical monitoring at their own milieu. Administratively, this benefit put hospitalization system in great change that patients freed from traditional wire system attached to bedside, make possibility of mobility of patient , decrease crowd and need of more beds in hospital , easy transferring of patient from surgery rooms to other places and made pervasive monitoring system in whole healthcare domain. Secondly, this system provides more efficient treatment in internal hospital environment. Because, BSN provide more data quality, accuracy, data resolution and integrity of computations as compared to traditional systems. Wearable systems focus on early detection and prevention of disease and it provide optimized maintenance of all disease. This system provides preemptive network with significant optimal and accurate monitoring and diagnostic milieu of life-sustaining signs. It also provides a real time feedback to medical professionals and users.

2.1 Architecture of BSN

There is a long application address list covered by BSN that provide achievement pillar to medical care system. From last decade mainly following application developments and devices introduced by BAN in health care system. These are "MobiHealth, Code Blue, Artificial Retina Epileptic Seizures, Hip Guard system, Ubimon, Strike Early Warner, Smart Life Shirt, eWatch, Vital Sign Monitoring System," etc. However, the requirement of WBSN leads to more and more

effective research in near future. The improvement herein area comes about 1995. Afterward on 2001, this technological area formulate for name like as body area network. Here in BSN biosensors place inside, outside, close to or as needful to human body in such a manner that they collect data, make possible operation on data, exchange information with each other and process signals if assimilation required and send information to the Base Station (BS). Research shows that there is much structural architecture defined for BSN however particularly it can be divide in three major parts. Sensors that are placed on patient form a separate network, high and lofty memory as well as processor units named as base station (BS) or Gateway (GW) and external cloud of network which also consist of medicinal servers and other terminals. Medical sensors that are attached to patient putted in such a way like: by stitching, wear or hang them, by surgery inside the skin, as required by the physician. Sensors that are attached with patient communicate to GW as they make change in data or after specific time. GW controls all body sensors and transfer information to external network. Patient data is stored on at external servers or network. Physicians/Doctors after log-in their server read and manipulate reports. Medical server also make possible reports and result upon data collected of patient.

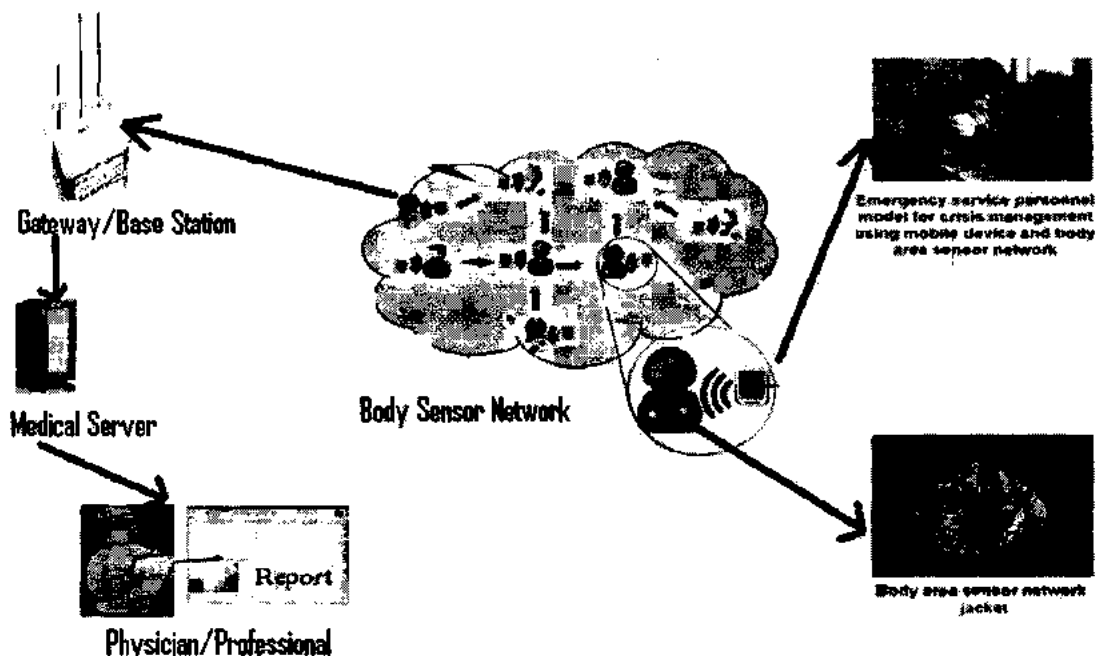


Fig: 2.1 Body Sensor Network [5]

2.2 Body Sensor Network's Requirements

BSN has got significant attraction in this century. Various uses of BSN being formulated for further simple and valuable to make part for such milieu like Health measurement, telemedicine, physical activity and convenient multimedia system. Because of improvement in MEMS expertise and sensor area compose BSN further motivating and practical for personal life, therefore it became a successful development area. Fundamentally, BSN composed real health management and recovery system [1]. Utilization of BSN classified two main categories: as health and non-medicinal applications. Bio sensor / Medical sensors are putted on person body to verify the person's health behavior such as Temperature, Blood pressure; pH monitor, Examine of Cardiac arrhythmia, and Brain liquefied pressure examine [11]. Some other sensors that directly can't took part in medical measurement however they used to communicate other biosensors or just used as for formation of network and for manipulation of result.

2.3 Challenges for Body Sensor Network

BSN is emerging novel era having many problems need to solve despite of all development and solutions in health care system. These challenges not only highlighted main points but also provide new beams in this particular area for researchers. Some of those topics are:

- **Interoperability:** WBAN should make sure flawless data movement over multiple standards such as ZigBee, Bluetooth etc. to endorse data exchanging, plug and play mechanism interaction. Furthermore, it ought to be scalable, guarantee competent movement across network and make continuous connection building.
- **System devices:** The devices used for BSN should provide low complexity, tiny in form factor, lightened weight, power proficient and reconfigurable. Further, remote storage facilitation and patient data's access via external processing would be required.
- **System and device-level security:** Significant effort must require for BSN to make communication secure and truthful. Patient data's privacy and authorized access for network and servers would be needed on each and every cost.

- **Assault of privacy:** Public might thought about the BSN machinery as a probable hazard of sovereignty, if applications found unsecure on different channel of medical usage. Social appreciation probably good for this area to resultant a progressive application.
- **Sensor validation:** All-encompassing schemes are question to innate communication and hardware factors including untrustworthy wired/wireless infrastructure, interfering and restricted power resource. This caused to invalid datasets being communicated back to the end user. In healthcare domain so it necessary for devices data validation. This helps to identify many possible delicacies in hardware or software design.
- **Data flexibility:** Information located on numerous portable devices and body nodes need to be composed and analyzed in a picture perfect manner. Inside BSN, serious patient datasets fragmented over different terminals and across a network of other small Wi-Fi terminal. So, if a medicinal practitioner's terminal does not enclose all recognized information then the superiority of patient care might be degraded.
- **Interference:** BSN connections are wireless therefore it ought to diminish the interference and amplify the coexistence nodes to other available nodes in the milieu. Effective implementation of BSN especially needed.

Above and beyond appliances-centric threats, some consumer-centric threats ought to be measured for realistic BAN advancement. These may include

- **Cost:** Today users may look for squat charge health metrics and solutions those also offer lofty functionality. BAN implementation should be cost reducible for tempting alternatives to health aware consumers.
- **Continuous Monitoring:** Each user require special level of monitoring, those who at threat of cardiac ischemia should need WBANs to be report constantly, while others may just need to monitor for walking or physical movement. The intensity of monitoring authority, energy required and life of BAN earlier than power source should be destitute.
- **Unswerving Efficiency:** The efficiency and performance of BSN ought to be unswerving. Sensors dimension have to be perfect and determent when ever as BAN switched off or on

again. Wireless connections have to be healthy and should be work beneath a variety of user environments.

Regardless of above mentioned challenges/issues some major are disclose in bellow section. One of these is considered and focus in this thesis.

2.3.1 Placement/Implementation Challenge

The placement of BSN nodes is ubiquity because of their energy requirements. These devices placed inside the body or wore on the patient body. In some inside placement environment these devices may raise issues for no replacement as well as implementation. Furthermore, when these devices transmit data to other nodes that nodes may be heterogenic or homorganic for other nodes in the environment.

When specially taking to the heterogeneity of devices then it also make impact on other issues. Specially, [32] it increases energy consumption and resultant the lifetime of network decreases. Because of that every type of device has its own processing capability and architecture. So, deployment of medical devices as implicated in the restricted environment for medical data manipulation, many novel challenges arise. Therefore a generous research is obligatory to defeat these limitations.

So, deployment of medical devices as implicated in the restricted environment for medical data manipulation, many novel challenges arise.

2.3.2 Fidelity Challenges

Reliability or in other word Fidelity problem crop up in BSN for the restrictions of energy & portability of devices, focal challenges are expressed here as in [5],

- Reports and result of BAN are directly alarm to human being, manipulation of reports derived from data collected through network environment, thus BSN require being extra consistent [19].

- The major characteristic of BAN include that their unidirectional paths exist from sensor to descended [5]. Topology infrastructure can also fluctuate caused by link crash, power breakdown or mobility of nodes [20]. So it needs more fidelity for better performance.
- Although we consider unrestrained battery life, the improved communication power gives outcome in damage of the skin [5]. Therefore, trustworthy network need to be ensure.

2.3.3 Security Challenges

Security is very critical to keep guard individual data beside illegal entrance like eavesdropping, DoS attack and alteration of message. Biomedical data particularly in m-health and telemedicine should be protected because it is very susceptible and illegitimate user may use for spiteful purpose or for deceptive accomplishment that can root to momentous yarn to enduring life. This exercise may lead to a false treatment and also may keep away physiologists from the root cause of any disease. Also if treated the chronic disease in such environment then effortless result occurs in diagnosing of track of chronic.

Normally, it is impracticable to apply conventional protection mechanisms to tiny biosensor nodes. However, BSN security challenges are mostly same as used for traditional WN, that are availability, confidentiality, integrity of data, authentication on accessing the system, freshness of data to evade from alteration of data and non-repudiations. True speaking, it is concluded that it is very complex and grave issue to launch historical protocols in BSN applications.

There are a lot of methods and mechanisms introduced in WSN to cope on the essential security threats. These exercises accomplish not only their required target but also provide beam for researcher that they can make potential enhances to in previous schemes to cope the challenges more efficiently and beautifully. These methods further applied new era of WSN that is BSN to achieved significant result not only for security but also for devices new trends like tiny, resource, less computation and transmission scenario. In this thesis we also try our best to introduce a technique for BSN keeping in mind of limited resources of devices which is more significant and strong in this new era and it also open novel methods in coming research mechanism in BSN.

2.4 Key Concord in BSN

Key management protocol is the heart for protected communication using cryptography. Bio Medical Sensors contain susceptible character of information hence it aggravates safety measure and challenge. The main task of key management is to build secure associated channel for neighbor network nodes, to ensure that all information will exchange in multi-hop scenario. Key management provides efficient security for flawless communication between entities for a common or fastidious session. As we are familiar that well-built cryptographic manipulation should be needed for higher wealth like memory, energy and bandwidth, thus it is mainly tough job to go for suitable cryptography system for resource limitation MBS that can provides more security using after that minimum resources.

Normally key management/encryption decryption mechanism in cryptography has two main types that are Symmetric and Asymmetric. Asymmetric crypto scheme or PKC contain two keys one is (public) for encryption and other one is (private) for decryption. Well known systems are RSA and Diffie-Hellman having reward about scalability and security however both are costly that have problem for key storage, maintenance are main issues for MBS. Another one ECC have advantage over RSA for less key size. Symmetric crypto systems have only one key for whole system it is good for tiny devices due to its small size of keys but have security and dynamic environment problems mean to say not versatile enough. Despite of pros and cons of both schemes in BSN it is supposed to be careful in selecting key scenario and keep some important factors in mind which are: Energy: Power needed for computation and communication for a certain number of bits and data. Memory: That is mean by temporary or fixes space require for computation and key/data storage. Time factor: As data size will be low than less time will require for computation or transfer so how much time hold by any one scheme?

To triumph over the high cost of PKS and security and dynamic issues of SKS and gain reward of both methods we here introduce a hybrid approach. Which will provide authenticated key agreement in BSN with rekeying scenario and that gave significant results for MBS implementation scenario.

3

LITERATURE SURVEY

3. Literature Survey

BSN is a new emerging study area from last a decade and numerous researches have been made and at a standstill new ideas are coming day by day to compose this era more useful and important. In this study we try to thrash out different ideas introduced and published for BSN earlier. Security and key management mechanism is heart of our thesis study due to its importance in human life in BSN. Multiple key management schemes are gone through in our study and achievement and lacks of these schemes are high-lighted and summarized. In symmetric cryptography schemes, sharing of keys mechanism in BSN needed a pre-loaded or pre-distribution scenarios. At the end key technique that coined for my thesis is discussed.

3.1 Different Published Scheme's Review

Mainly those papers are reviewed here that are closely related to our work.

[1], [2], [3] schemes used a pre-shared method where that secure key already known among each node that is loaded. Nodes after deployment create another key using security protocols for a time frame session. These types of ideas are very practical for large and huge environmental network, where fixed or non-scalable technique is used. However, such type of methods can't sustain dynamic milieu. Addition, revocation, updating of membership and then to make computation for group keys whenever needed is not practical and very daunting task in these methods.

Another method in, [4] put some better mechanism using SKC, where PKs used to protect the SKs distribution in Ad-hoc network. This scheme guaranteed higher security in SKs sharing. Author used PKs that protects SSK which is distributed among sensors. On the other hand, this method is not suitable for BSN because of high cost and computation doubled by introducing combined method of PKS and SKS.

A novel biometric method [5], introduced bio channels for key sharing. These bio channels that in fact pathways used for key sharing. Any biological conduit taken borrows from available channels for key managements. Problems occurred on dynamic behavior nodes for GRKs by bio-metric system. Hardware Encryption scheme also used for some architecture. But

this is not efficient due to high cost at manufacturer level as well as when replacement of equipments is needed.

The WBAN [6] and ALARM-NET [7] brought mechanism in which designated server responsible for key distribution among network nodes. It formulate on basis of AES encryption standard hold by CC-2420. Here CBC, CCM and MAC authentication and encryption performed. Drawback of these approaches is of special platform like hardware depended schemes and only base station capable of doing decryption. Intermediary nodes, if want to decryption for any purpose they can't to do so.

ECG or physiological signals also used for key generation and management. Referenced idea number [8], used a novel IPI method for creating secure keys. Time differentiation calculated using altitude of PPG or ECG signals. 128 bits size key is then generated after making necessary calculation. Hamming distance is also calculated for error detection and makes possible correction in transmitted data. Random method for keys scenario is used therefore the performance of technique is efficient. Conversely main disadvantages for this idea are; first one is that IPI values extracted at different terminals have small difference therefore error correction code must require for keys equalization. Secondly, as data rate is being very high due to BSN environment therefore slow mechanism is considered for keys formation.

Another method that performs MS relationship among nodes is the RDP [9]. Usually one device become as master and maintains policies for other communicating devices according to the network scenario. Drawback occur when disassociation of sensor is sensed in network, the devices that freed from previous patient does not properly associated with the network and no solution is defined well to make reusability of device properly. Therefore this approach is not successful for a large and sudden react hospital system.

Jiang et al. [10] established the pair wise key mechanism for authentication using ECC and SCK. A KDC must need here to load information on sensors securely and then based upon IDs devices commit to KDC for authentication and information sharing. To carry out authentication, user is required to reveal the association of shared secret key for as a minimum t sensor. Relationship then achieved, if distinct ECC parameter be measured for each patient in

BSN. When sensor to patient relationship could not form in efficient manner then flaws for such approaches beamed for security and structural deployment mechanism.

SNAP [11] defined an architecture where ECC is derived for pair-wise key establishment along with node and base station. A Biometric device is used that affixed to each patient for sensor and patient authentication and that is also used for shared secret keys communicated by base station to the participating devices. The lack of this method is that group key requisition is not performed and all authentications are carried through base station. Sensor then required more memory and energy for again and again request about authentication and key requisition.

Many works have been done to address key management using ECC. [12], also uses fields to measures key management for ECC curve parameter. It also leads to resource constrained for BSN. All method does not support for fresh keys, node adding up and revocation scenarios in key management aspect.

Dimitriou et al [13] article planned several security scenarios to protect bio-medical sensors network. That is Tiny Sec: which provide link layer security, and also achieved link layer encryption and authentication of susceptible data. The limitation is that it only gave a base line security, and cannot keep guard beside attacked node.

In [14] author jointly used ECC secure system and TCG manner to realize healthier performance because of TCG is efficient method for management of keys securely for servers that are communicating in system and ECC stand still strong mechanism for distribution. The RSA and ECC compared here according to their performance. The major limitation of proposed idea is that it is difficult to requisition for more sources because ECC used long keys for message encryption.

The proposed methods in [15] and later in [16] are the main basic paper for proposed idea. Authors here in [15] proposed a good approach for key agreement and efficiently used rekeying scenario by launching the PKC scheme, here author used RSA and DHECC parameters for whole key management protocol. Rekeying features provided here with key addition and revocation options that is suitable for dynamic scenario of WSN. Same method of author also introduced in BSN. Scalability, better dynamicity and resiliency achieved here by using

particular routing scheme in keys agreement practice. However, limitation comes for this scheme by using both RSA and DHECC that takes more memory and needed higher processing power for computation cost. Holding both PKC methods still an issue for minute devices that are especially used in BSN concerning to memory, communication and computation cost.

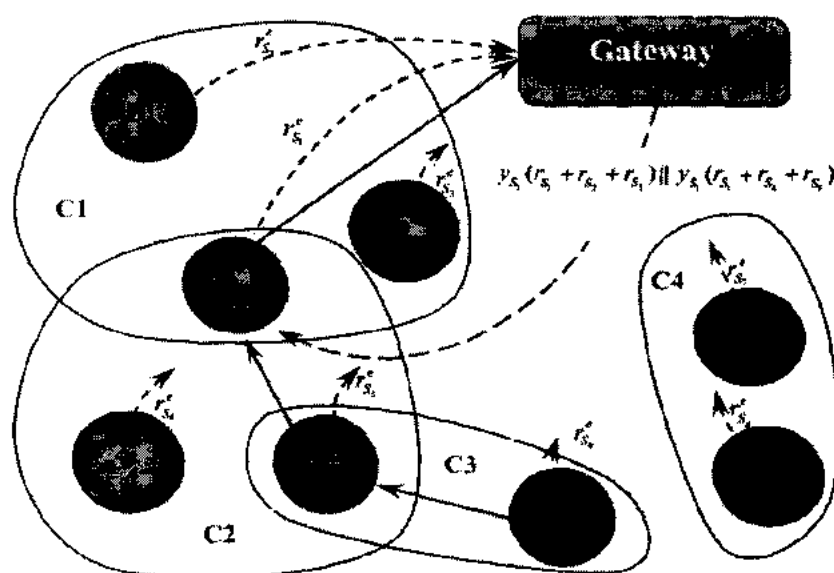


Figure 3.1 Key management models of [15]

In [16] author introduced an optimized computed algorithm of RSA implementation. The implemented scheme efficiently utilized that gave proves of PKC that is effectively practical in WSN. Authors, modifies packet format and implement the cluster scenario. Decryption of message is only performed on BS. CH stores PK of BS and node stores PK of CH. Implementation done by using NS2.34 and results produced by taking different energy threshold values. Results increases network life time. However this scheme not efficient in BSN due to PK storage and whole domain mechanism encryption procedure. Due to usage of PK for both CH and node there are issues of communication cost, memory and computation cost. Using PK in such scenario CH congested. Also rekeying process didn't used here.

3.2 Review Conclusion

As we examine different methods and their contributions and limitations relating to key management in WSN/BSN. As in MBS have limited resources so PKC can't be useful openly because it need more energy. Schemes, in which PKC applied, are not an optimal solution for tiny devices. Other one SKC when applied may best for tiny devices but have own restrictions. Besides their disadvantages their contribution is also good gave beam for new ideas.

In our novel idea we introduced hybrid approach in a new and efficient manner for BSN. This will cover not only the limitations of previous hybrid and other approaches but also guarantee for more security, reliability, scalability and freshness of data and keys to personal healthcare system.

4

PROBLEM STATEMENT

4. Problem Statement

After going the thorough study of different approaches that are elaborated in above literature work, deficiencies that are mentioned against each scenario need to be address in term of optimal solution in some better manner. The main objective is how; we can efficiently manage power to get better life of nodes, scalability, and security for BSN. As security is essential discussion for our thesis and in BSN the heart for safety measures is key management. Multiple keys management techniques are observed in above study. Mainly the mechanism is based SKC or ASC.

In different methods of PKC [5], [6], [7] for legitimate keys agreement in BSN normally, RSA and DHECC used. These schemes consume more power and have higher computation cost due to large keys sizes is RSA used 1024 bits and DHECC used 160 bits. Not only above but these have lofty communication cost because of Enc. and Dcn. taken place on each node and data is transferred in high bulk scenario e.g. ten nodes are there so there will be ten PKE and PKD. And if consider just only 160 bit key size then after manipulating with a sufficient data size then packet size increased along its magnitude as data high. So as data magnitude rises then as much energy will be needed.

Taking about Symmetric key cryptosystem it is judged that the mobility and portable requirement scenario of SKC has lack of revocation, addition and deletion of nodes [15] that is normally introduced in each and every novel technique.

So closing the discussion we can say that Asymmetric scheme for authenticated key agreement in Body Sensor Network consumes more computation cost, communication overhead and required additional memory [5], [6], [7] for key storage. Symmetric schemes for authenticated key agreement have lack of dynamic environment [15] and scalability [15].

4.1 Propose Structure

We introduced a fresh hybrid authenticated key agreement for Body Sensor Network with rekeying scenario, to over-come the lacks of PKC from node side in term to save energy and memory, and to achieve greater security and scalability with rekeying and freshness for SKC. The proposed technique composed of ECC and symmetric scenario.

The main burden of PKC is on Gateway side that have no energy problem and have high resource. Here we place three patient network model. Each patient shown with number of bio-sensor and the bio-sensors of each one patient figure a cluster base scenario. Partially, no need for CH selection and communication is carried out to each nearer cluster to its neighbour for other body virtual cluster. Here is also a GW, which is a fundamental device between BSN and MU. As GW has a high resource therefore no one ceiling to control and manage different scenario and operation for GW. GW finds the routing Path-Table accordingly [13], [14] to depend by deployment information of devices and store cluster structure circumstances using optimized route-selection procedure. The collected data of bio-sensors are forward to MU through GW. The propose scheme consists of three phases.

- A. Keys Pre-loading Phase
- B. Session Keys Setup Phase
- C. Re-Keying Phase

The detail of proposed model is written in section 5.

4.2 Scope of Intended Solution

Proposed scheme is a novel method for BSN that is based on PKC for calculation and maintenance of keys and on SKC for medical data transitions from nodes to GW. Result and calculated analyses realize that our scheme is more proficient.

4.3 Research Purpose

The key objective of proposed research idea is to corroborate and evaluate fresh security technique for competent and protected communication in BSN to attain low computation cost, communication cost, and memory storage that also grantee better security. Our proposed scheme will firmly manage and distributed key among nodes in BSN.

4.4 Role of Research

After study of the of security requirements of BSN, and after analyzing the restricted resources of such unique network, and multiple proposed work for the security require of BSN, we after that introduced a novel technique that in some way contribute in this field by reducing its main lacks and provide efficient results. And hopefully our scheme significantly contributes in the field keys management and security in particular in BSN in future.

5

PROPOSED METHOD

5. Proposed Mechanism

Our proposed keys-management scheme provides better and complete solution for said problem that is discussed in above section. Because propose mechanism cover all phases of said problem relating to security and keys authenticity. The intended feature of proposed mechanism is explained in this section.

5.1 Designed Marks

Our propose scheme “A Hybrid Approach to Authenticated Key Agreement with Rekeying for Secured Body Sensor Networks” has following characteristics.

- To capture benefits of both SKC and AKC.
- Should be efficient and result oriented as compared to traditional methods.
- It will increase network life-time and save node energy.
- Should scalable and dynamic with authentication.
- It ensures better security and keys management.

5.2 Proposed Scheme Structure

To prevail over the high cost of AKC we introduce hybrid technique for session key exchange. Our novel method setup session keys between nodes and among group nodes realizing authentication of devices and consumers. Hybrid technique used ECC and symmetric cryptosystem.

Structural model for keys based on Elliptic curve and symmetric cryptography. In this scheme we assume that GW has high energy, memory and processor capabilities. Gate-way formulates the routing Path-Table according to [13], [14] depend by deployment information of devices and store cluster structure circumstances using optimized route-selection procedure. The proposed model constituted on three phases; before installation keys pre-loading phase, session keys-establish phase and rekeying phase. Whole scenario of scheme is exposed in Figure 5.1. Sensor nodes that are placed on patient form a separate cluster for each patient that belongs to that are P-1, P-2 and P-3. Sensor nodes that are in communication way but belongs to different patient form separate clusters that are C-1 and C-2. Gateway is resource-rich and responsible for to construct the routing Path-Table and send data to network. Further medical professionals generate reports

logging on the medical server and diagnose upon their report. For easiness of study, these notations we used in this model.

5.3 Terminologies

Notations that are used for easiness of understating in this thesis are listed and organized here in below table.

Table 5.1 Planned Technique Notations

Notation	Description
q	A large prime number ($q \geq 2^{160}$)
C	An Elliptic Curve over prime field F_q of order q
G	Point of order ($n \geq 2^{160}$) chosen from points on C
d_{gw}	Gate way GW private key
p_{gw}	Gate way public key
ID_{si}	Identification of sensor S_i
ID_{gw}	Identification of Gate way GW
r_{si}	Randomly select number
k_{pi}	The shared key for the patients in cluster i
k_{Cj}	The shared key for the shared cluster number j
E_k	Encryption with key k
D_k	Decryption with key k

The overall structure and model of our proposed scheme is designed as below in diagraph. This model clearly defined and picturized the whole scenario as well as flow of communication. According to the bode sensor network structures, sensors are shown here on the body and each body makes a culster of implanted sensors that it uses. Therefore, here in this model mainly three culster are shown as there are three bodies that on sensors are placed. Out of these three cluster the sensors that make communication between these cluster form separate cluster for communication purposes.

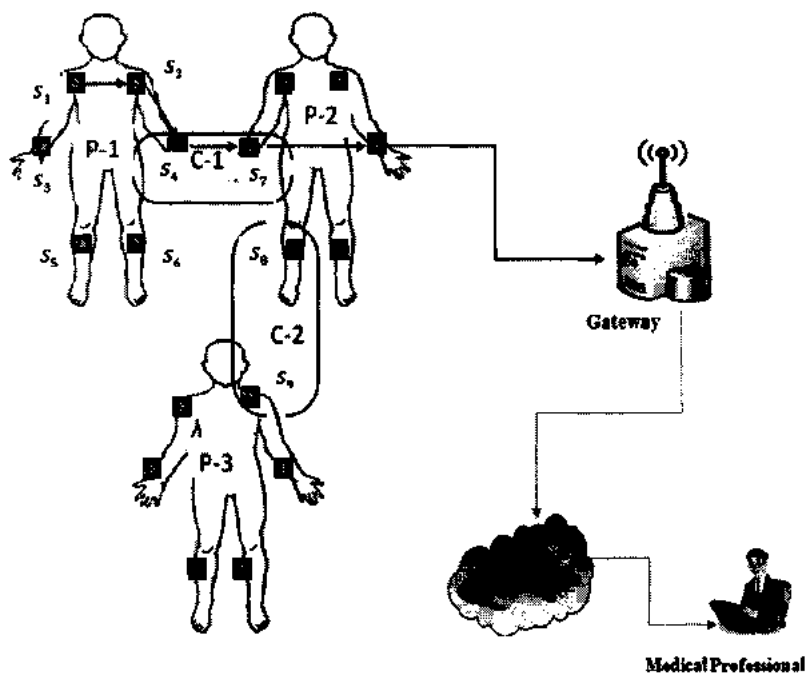


Fig: 5.1 Proposed Scheme Network Infrastructure [31]

5.4 Proposed Methodology

These are the three central phases conceded out in our hybrid mechanism.

5.4.1 Keys Pre-loading Phase

In first phase each one sensor S_i is pre-loaded through GW public key. GW also pre-loaded with its own private and public keys and each sensor S_i ID $_{S_i}$. Table 5.2 holds the saved keys that are placed before deployment on GW and Sensor S_i .

Table 5.2 Pre-loaded keys phase

GW	d_{gw}, P_{gw}
Sensor S_i	P_{wg}

5.4.2 Session Keys Setup Phase

Session keys are constituted in BSN according to the practice portray in Table 5.3 and exemplified in the Figure 5.2. Gradually course of action is detailed in this section. That shows keys formation process.

Table 5.3: Key Establishment

$S_i \rightarrow GW$	$E_{P_g}(r_{si} \parallel ID_{si})$
$GW \rightarrow S_i$	$E_{r_{si}}(k_{pi} \parallel ID_{si} \parallel ID_{gw})$
$GW \rightarrow S_i$	$E_{r_{si}}(k_{Cj} \parallel ID_{si} \parallel ID_{gw})$
$S_i:$	
	$D_{r_{si}}(k_{pi} \parallel ID_{si} \parallel ID_{gw})$
	$D_{r_{si}}(k_{Cj} \parallel ID_{si} \parallel ID_{gw})$

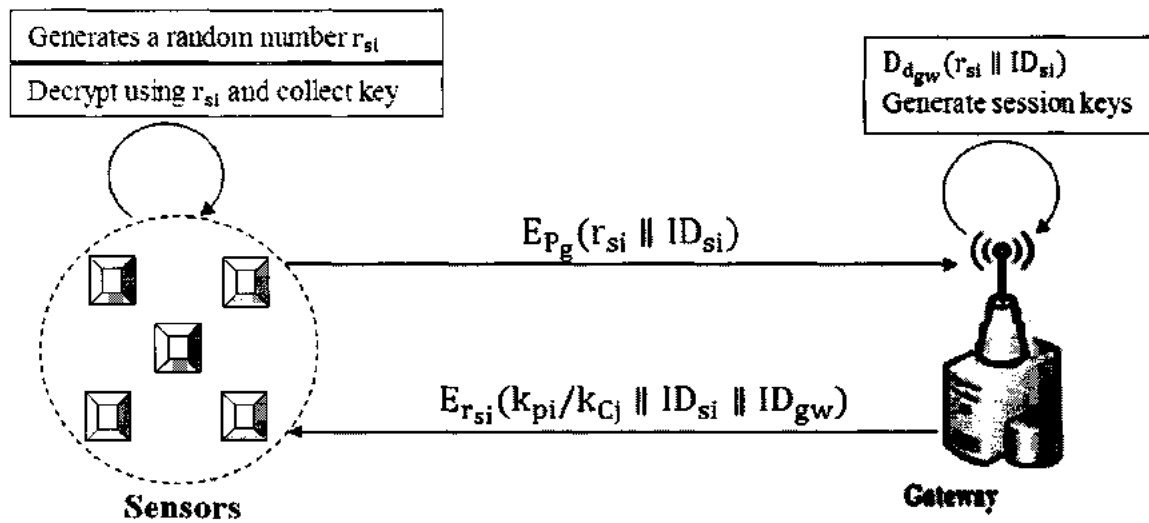


Fig: 5.2 Session Key Establishment

Accession No. TH13155

5.4.2.1 Session Key Establishment Phase

1. Each sensor S_i generates a random number r_{si} concatenate with its own id ID_{si} , encrypt with gateway public key using ECC encryption and send to gateway GW.
2. Gateway decrypt the information received from sensor S_i and $r_{si} \parallel ID_{si}$.
3. Compare received ID_{si} with stored ID_{si} for integrity of received information, as integrity is achieved through avalanche effect.
4. To generate session key for cluster P_i , gateway select two r_{si} from those sensor S_i r_{si} 's belong to same cluster p_i .
5. To generate session key k_{pi} , gateway take XOR two r_{si} belong to same cluster i
6. To Generate session keys; k_{Cj} , for cluster C_i gateway take XOR of two r_{si} randomly belongs to same cluster j
7. The gateway established session keys k_{pi} and k_{Cj} with sensor S_i , gateway use symmetrically encrypt k_{pi} and k_{Cj} using r_{si} as key.
8. Each sensor S_i decrypts the received information by using symmetric decryption and key r_{si} .
9. Compare received ID_{si} with stored ID_{si} and ID_{gw} with stored ID_{gw} for integrity of received information, as integrity is achieved through avalanche effect.

5.4.3 Re-keying Phase

Freshness of data and key is essential in security scenario. So, when a sensor joins or leaves the system or later on a specific point in time for freshness of data rekeying process is initiated. Each sensor S_i generates a random number r_{si}' and the similar practice carried for next keys k_{pi}' , k_{Cj}' as in establishment phase. On the other hand GW cross match previously used numbers and IDs for authenticity. Here given below table and graphical scenario elaborates the whole procedure for this phase.

Table 5.4 Re-keying phase

$S_i \rightarrow GW \quad E_{P_g}(r_{si}' \parallel r_{si} \parallel ID_{si})$ $GW \rightarrow S_i \quad E_{r_{si}'}(k_{pi}' \parallel ID_{si} \parallel ID_{gw})$ $GW \rightarrow S_i \quad E_{r_{si}'}(k_{Cj}' \parallel ID_{si} \parallel ID_{gw})$ $S_i:$	
<table border="1"> <tr> <td> $D_{r_{si}'}(k_{pi}' \parallel ID_{si} \parallel ID_{gw})$ $D_{r_{si}'}(k_{Cj}' \parallel ID_{si} \parallel ID_{gw})$ </td> </tr> </table>	$D_{r_{si}'}(k_{pi}' \parallel ID_{si} \parallel ID_{gw})$ $D_{r_{si}'}(k_{Cj}' \parallel ID_{si} \parallel ID_{gw})$
$D_{r_{si}'}(k_{pi}' \parallel ID_{si} \parallel ID_{gw})$ $D_{r_{si}'}(k_{Cj}' \parallel ID_{si} \parallel ID_{gw})$	

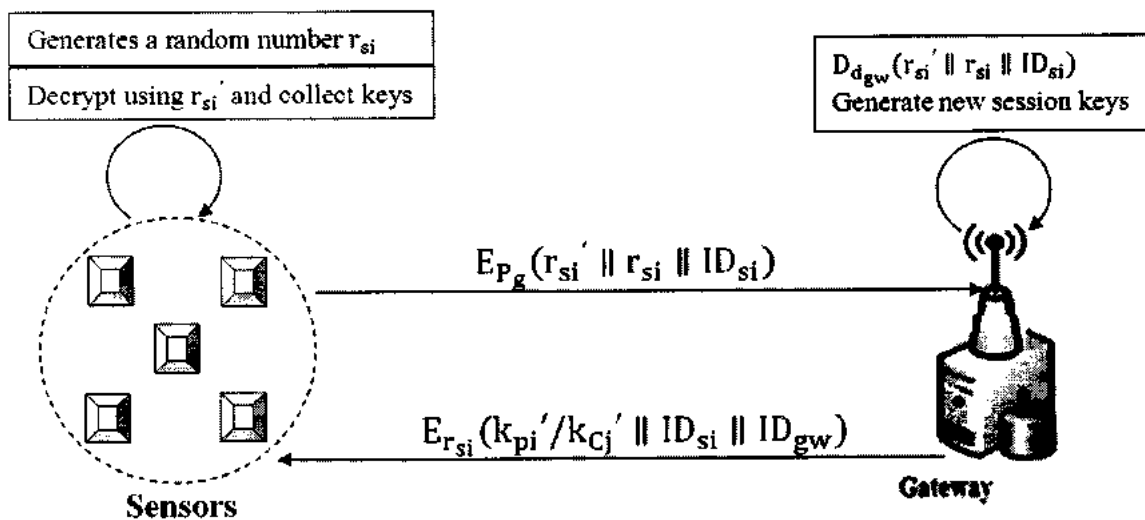


Fig: 5.3 Re-keying phase

The mainly difference between the key establishment and rekeying phase is that in rekeying phase older keys and IDs of nodes also considered using their random number generation keying process.

6 SIMULATION AND MATHEMATICAL RESULTS

6. Implementation And Results Validation

Chapter includes the detail discussion relative to simulation scenarios. The proposed scheme based on the simulation of network model and mathematical fundamentals. Multiple scenarios and test cases generated on the different values according to standards of BSN and WSN. In simulation assumed a specific number of nodes and their energy. In mathematical model assumed mathematical calculation for results. As energy is main source of sensor node so our work focused on sensor energy and as we know that GW is rich in resources. The analysis of scheme will be validated according to NIST key standard and other performance measures platform.

6.1 Simulation

In 1996-97, work on (ns-2) was initiated based on a refactoring by Steve McCanne. Use of Tcl was replaced by MIT's Object Tcl (OTcl), an object-oriented dialect of Tcl. The core of ns-2 is written in C++, but the C++ simulation objects are linked to shadow objects in OTcl and variables can be linked between both language realms. Simulation scripts are written in the OTcl language, an extension of the Tcl scripting language.

6.1.1 Simulation workflow

Simulation is divided into several steps for general purpose:

- a. Topology definition: to ease the creation of basic facilities and define their interrelationships, ns-2 has a system of containers and helpers that facilitates this process.
- b. Model development: models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.
- c. Node and link configuration: models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system.
- d. Execution: simulation facilities generate events, data requested by the user is logged.

Table 6.1: Simulation Parameter for BSN *IEEE 802.15.6*

Simulation Parameters	
Parameters	Standards
Topology_ area	(500 x 500) meters
Node numbers	05~20
Antenna_ Type	Omni Antenna
Connection Type	TCP
Initial_ energy	10J
Data_ packet_ size	30 Bytes
Processing_ power of sensor node	5nJ/ bit
Tx_ Power	36nJ / bit
Network Components	Link Layer (LL), Interface Queue (IfQ), MAC layer
Channel Type	Wireless
Physical Type	Wireless Physical
Rx_ Power	36nJ / bit
Frequency	9.14e+08 (914 Mhz)
Hr_ Height of Receiving Antenna	1.5 meter above ground level
Ht_ Height of transmitting Antenna	1.5 meter above ground level
CSThresh_ Carrier Sense diameter	1.5 meter
Bandwidth_ data rate	2Mbps
Routing_ Protocol	AODV
Agent_ Trace	ON
Movement_ Trace	ON

The above table provides the detail relative to the parameters that are used in our simulation scenario. Generally speaking about the standards frequency that 802.11.5 [34], BSN has used the frequency band of 2.4GHz for its compatibility with the existing wireless communication standards such as Bluetooth or UWB [34]. It can transmit the signal to the relatively long distance, ~10m. But, its energy consumption for the communication is relatively high, the order of nearly 10nJ/bit. The <50cm distance in-body communication system supports low speed data rate, ~100bps, with 430MHz carrier frequency. The short distance, <5cm, through-body communication between implanted device and external read-out terminal can support Mbps data rate using inductive coupling of 415MHz carrier.

Here in Ns2.35 simulator, by default it uses values according to Phy/WirelessPhy network interface type and from this also some assumption values also are set. However, these values can be changed to achieve the better results of simulation. In our scenario we set here frequency as $9.14e+08$, means that of 914 MHz by default. The height of transmitting and receiving antenna is 1.5 meter above the ground level for nodes. And the carrier sense for incoming packet is at distance of 1.5 meter away from the node. We also used 2Mbps data rate to transmit the packets. For the assumption of processing power of sensor node we used as in [16], the processing power of sensor nodes is 5nJ/ bit.

6.2 Result Validation

Simulation result and Mathematical computations has been made here and their graphs are explained. In each graph and table previous scheme named M. Hamdy et al and our proposed schemes result has been compared.

Our proposed scheme simulated by NS2.35 network simulator and Fedora operating system is used. Proposed model consists upon 5 nodes, 10 nodes, 15 nodes and 20 nodes in different attempts for comparison of results.

6.3 Cost Analysis

Whenever a security protocol is implemented then the energy impact of added security protocol must be considered. In this scheme we assume a specific energy for node and generated results for each requirement that are as follows;

6.3.1 Communication Cost

Communication cost as relative to energy rounds graph for sensor nodes is compared here through simulation as shown below. Our scheme clearly produces efficient result and consumes low energy as in different 5 rounds statistic. Our scheme uses less packet size through smart encryption key size and communication done upon considering different rounds. Our scheme consumes less power of sensor and it's this magnitude goes higher as rounds increases.

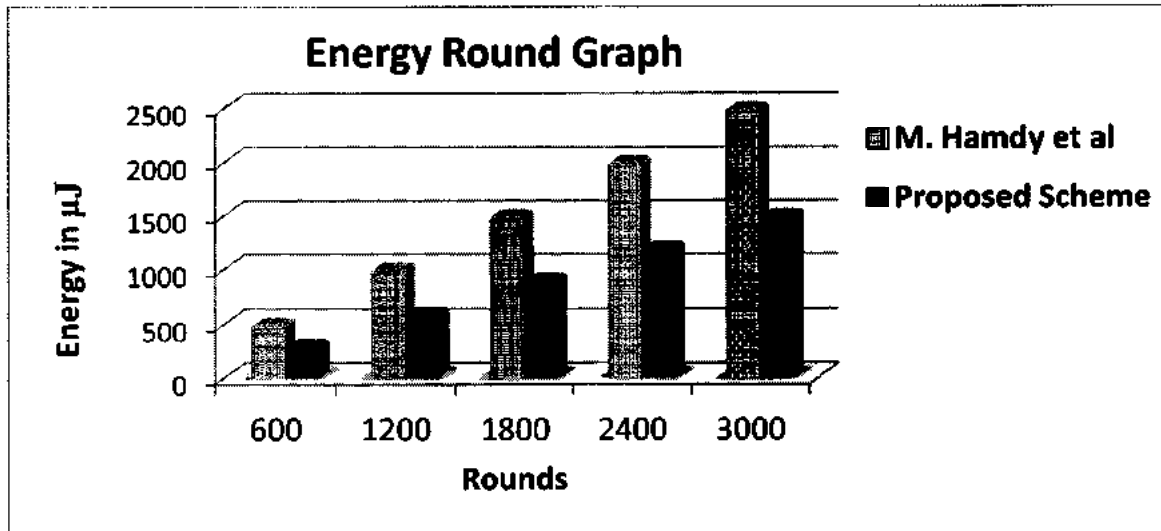


Figure 6.1 Communication Energy Cost for Different Rounds

6.3.2 Communication Overhead

Bandwidth is the major issue in body sensor network so less communication cost is of greater interest in BSN. In proposed scheme some nodes are considered and transmitted keys for each round upon different node size and the generated results has been be compared with existing scheme. It is clear from the simulation result that our scheme transmits less number of bits so the proposed scheme produced less overhead as shown in the figure.

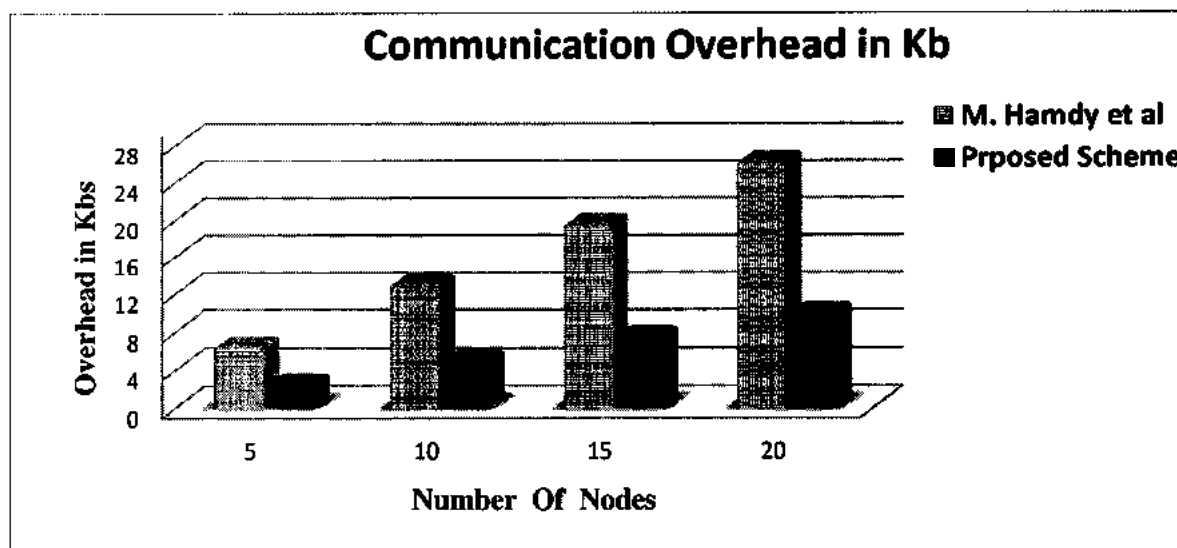


Figure 6.2 Communication overhead of key Management scheme

Table. 6.2 Communication overhead Reduction for Sensor [31]

Schemes	Communication Overhead	Communication Overhead Reduction in Percent
M. Hamdy et al [15]	(1024+320) bits	$\frac{1344-512}{1344} \% = 61.9\%$
Proposed Scheme	(320 + 192) bits	

6.3.3 Computation Cost and Key Computation Time Analysis

Modular Exponentiations or ME and Elliptic Curve Point Scalar Multiplication or ECPM are the costly and major operations in ECC session keys substitution. In scheme [15], author proposed both ECC as well as RSA for key exchange with two ME and four ECPM. Whereas our method just have only four ECPM. ECC 2^{160} Point Multiplication just takes 1.61 second while an RSA 2^{1024} private key ME takes nearly 22 seconds accordingly [22]. Accordingly these results we also save energy in Computation Cost as compare to [15]. Following calculation has been made and we saved 87.23% [31] time in seconds for key computation as compared to [15]. Results generated after simulation that also shows energy consumption of our and existing scheme. Taking to the specifically energy consumption of nodes according to the [16] the encryption and decryption energy consumed by the sensor is 6.22nJ/ bit for RSA scheme.

$$\frac{(2 * 22 + 4 * 1.61)s - (4 * 1.61) s}{(2 * 22 + 4 * 1.61)s} = 87.23 \%$$

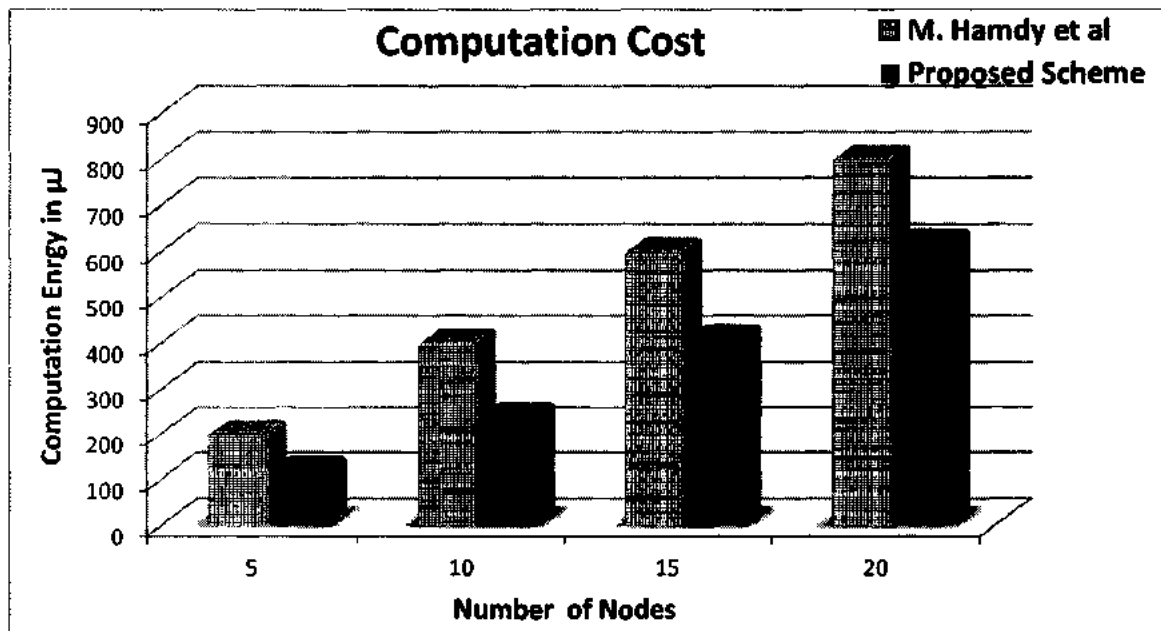


Figure 6.3 Computation cost of key Management scheme

6.3.4 Memory Requirements Analysis

As we know that sensor have limited memory therefore we implement such a strategy of security and key management that could consume miniature amount of storage space. As NIST recommended Key size for RSA, ECC and SKC, and taking supposition of ECC compress point representation, ECC has key length $\geq 2^{160}$, SKC normally for AES key length $\geq 2^{128}$ and RSA has $\geq 2^{1024}$. Analysis and result helps resources constrained nodes to save memory for further usage and if required for other purpose here our scheme gives good result according to calculation of [31] reduced 74% memory requirements upon a sensor and from graph we can see the difference of freed memory from previous scheme. Below table and graph shows the memory analysis result.

Table. 6.3 Memory Requirements for Sensor

Schemes	Key Stored	Approximate key size in bits	Percent Reduction in Memory Storage
M. Hamdy et al [15]	$d_{si}, P_{si}, k_{pi}, k_{Cj}$	160+160+ 1024+128+128	$\frac{1600-416}{1600}\% = 74\%$
Proposed Scheme	k_{pi}, k_{Cj}, P_{gw}	128+128+160	

The above table analysis shows that our scheme only used 416 bits key size for communication and the previous scheme whereas used 1600 bits key size for communication.

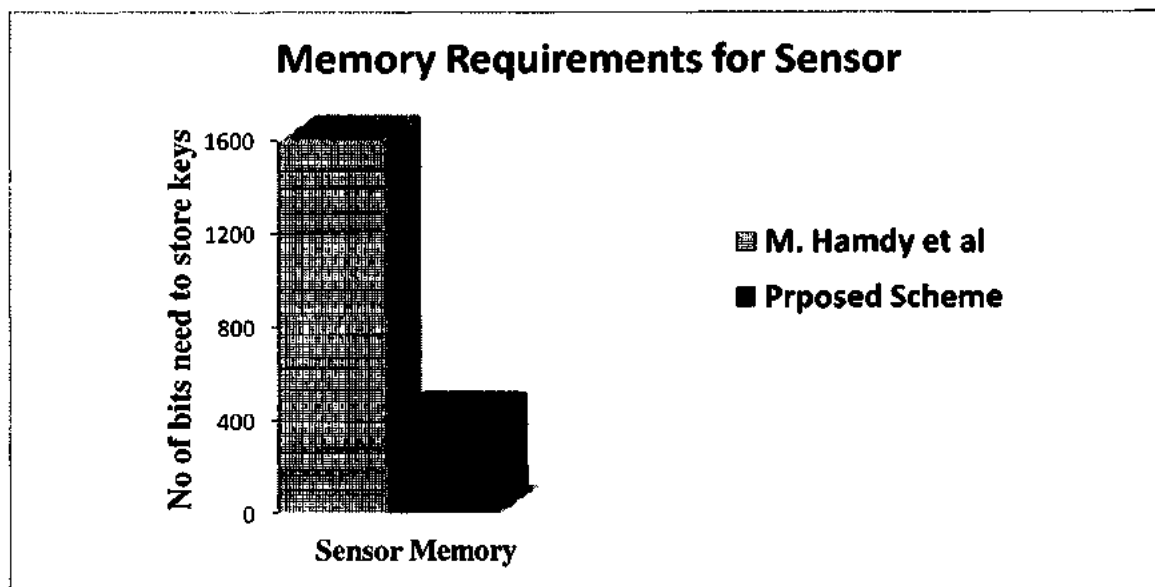


Figure 6.4 Memory Requirements for Sensor

6.4 Security Analysis of Our Scheme

Security of BSN data can't be compromise at any cost. So any of proposed schemes related to key agreement must ensure all fundamental scenarios of security threads. We also made analysis of security requirement of this scheme for Body Sensor Network.

Our scheme realizes to fulfill all requirements and ensure no one aggravates for any culpability upon devices misuse and data integrity. Following key point are considered for this analysis.

6.4.1 Confidentiality

Here we used hybrid approach in which ECC and AES used. As both schemes have confident key size against any attack and can't be challenge yet. Therefore proposed scheme has good resistance against any such attack. As these key sizes can't be captured so data communicated on network is full of confident against any attack.

6.4.2 Forward Secrecy and Backward Secrecy

As any bio-sensor that is used in the network have a unique ID so as a node leaves or joins the network or captured by some external attack then ID based system checks and ensures forward and as well backward secrecy.

6.4.3 Integrity and Authentication

When gateway performed any decryption then GW compare received IDs with stores IDs of nodes. And also sensor node compare received ID with stored ID of gateway. So both focal devices authenticate confidently. SKS and ECC both have avalanche effect that ensures integrity and authenticity maintenance.

6.4.4 Node Capture

As gateway's public key is pre-loaded in each sensor node and we believe that GW is skilled for detection of sensor node capture as in [23], if in any case not fond then our key refreshing mechanism will notify the compromised node, so as a result proposed scheme ensure enriched hardiness against node capture.

6.4.5 Scalability with Security

Extensive growth can be made in network size after deployment by rekeying mechanism. So our scheme ensures as required growth with good security requirement.

7 CONCLUSION AND FUTURE WORK

7.1 Conclusion

Key management protocol is the heart for protected communication using cryptography. Bio Medical Sensors contain susceptible character of information hence it aggravates safety measure and challenge. The main task of key management is to build secure associated channel for neighbor network nodes, to ensure that all information will exchange in multi-hop scenario. Key management provides efficient security for flawless communication between entities for a common or fastidious session. BSN is emerging novel era having many problems need to solve despite of all development and solutions in health care system.

To triumph over the high cost of PKS and security and dynamic issues of SKS and gain reward of both methods we here introduce a hybrid approach. Which will provide authenticated key agreement in BSN with rekeying scenario and that gave significant results for MBS implementation scenario. This will cover not only the limitations of previous hybrid and other approaches but also guarantee for more security, reliability, scalability and freshness of data and keys to personal healthcare system. Simulated and mathematical results shows that the proposed scheme save node's power and also provide efficient security against key captures and consume low power in communication and as well as computation cost.

7.2 Future Work

Our Proposed scheme is a novel method for BSN that is based on PKC for calculation and maintenance of keys and on SKC for medical data transitions from nodes to GW. Result and calculated analyses realize that our scheme is more proficient. In future, we will try this scheme some different scenarios like clustered based. Moreover the proposed scheme in future also applies it with the hash functions likely by using RC4, RC6 and other smart cryptography techniques for BSN Network as well as for data aggregation techniques and hopefully will be good according to security and dynamicity.

References

References

- 1) D. Liu, P. Ning, and R. Li, "Establishing Pair wise Keys in Distributed Sensor Networks," *ACM Trans. on Information and System Security*, vol. 8, no. 1, pp. 41 – 77, Feb 2005.
- 2) D. Liu, P. Ning, and W. Du, "Group-Based Key Pre-Distribution in Wireless Sensor Networks," in *Proc. ACM Workshop on Wireless Security (WiSe 2005)*, 2005, pp. 11–20.
- 3) L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. on Computer and communications security*. Washington, DC, USA: ACM, 2002.
- 4) A. Boukerche and R. Yen., "The Design of a secure key management system for mobile Ad-hoc networks," in *Proceedings of the 33rd IEEE Conference on Local Computer Networks (LCN'08)*, pp. 320–327, Quebec, Canada, 2008.
- 5) C.C. Y. Poon, Y. T. Zhang, and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.
- 6) S. S. M. Meingast and T. Roosta, "Security and privacy issues with health care information technology" *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5453-5458, Aug. 2006.
- 7) D. Singelee, B. Latre, B. Braem, M. Peeters, M. D. Soete, P. D. Cleyne, B. Preneel, I. Moerman, and C. Blondia, "A secure low-delay protocol for multi-hop wireless body area networks" *Ad-hoc, Mobile and Wireless Networks*, pp. 94-107, Sep. 20, 2008.
- 8) C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A Novel Biometrics Method To Secure Wireless Body Area Sensor Networks for Telemedicine And M-Health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.
- 9) F. Stajano, "The resurrecting duckling–What next?" In *Proceedings of the 8th International Workshop on Security Protocols*, Cambridge, UK, 3–5 April 2000; Christianson, B., Crispo, B., Roe, M., Eds.; Springer: Berlin, Germany, 2000
- 10) C. Jiang, B. Li, and H. Xu, "An efficient scheme for user authentication in wireless sensor networks" In *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, Niagara Falls, Canada, 21–23 May 2007.

- 11) K. Malasri, and L. Wang, "Addressing security in medical sensor networks" In *Proceedings of the 1st ACM International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments*, San Juan, Puerto Rico, 17 June 2007.
- 12) H. Wang, B. Sheng, and Q. TelosB, "Implementation of Elliptic Curve Cryptography over Primary Field" Technical Report WM-CS-2005-12; Dept. of Computer Science, College of William and Mary: Williamsburg, VA, USA, October 2005.
- 13) N. Lewis, and N. Foukia, "Using trust for key distribution and route selection in wireless sensor networks," *IEEE Globecom*, pp.16–30, Nov. 2007.
- 14) Q. Yang, A. Lim, S. Li, J. Fang, and P. Agrawal, "ACAR: Adaptive connectivity aware routing protocol for vehicular Ad Hoc networks," *Proceedings of the 17th IEEE International Conference on Computer Communications and Networks*, 2008.
- 15) M. Hamdy Et al, M. K. Khan, and K. Alghathbar "A Key Agreement Algorithm with Rekeying for Wireless Sensor Networks using Public Key Cryptography" *International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID)*, 2010.
- 16) A. Sahanaa , and I. S. Misrab. "Implementation of RSA Security Protocol for Sensor Network Security: Design and Network Lifetime Analysis" *2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE)*, 2011.
- 17) M. Hamdy Et al, M. K. Khan, K. Alghathbar, A. Tolba and K. Kim "Authenticated key Agreement with Rekeying for Secured Body Sensor Networks" *International journal of Sensors*, 11(6):5835–5849 mdpi. May, 2011.
- 18) L. Yao, B. Liu, G. wu, K. Yao and J. Wang, "A Biometric Key Establishment Protocol for Body Are Networks", *international journal of distributed sensor networks*, may 2011.
- 19) A. Peiravi, "Connectance and Reliability Computation of Wireless Body Area Networks using Signal Flow Graphs", *Life Science Journal*, 2010.
- 20) M. A. Ameen, A. Nessa, and K. S. Kwak, " QoS issues with focus on Wireless Body Area Networks", *IEEE Third International Conference on Convergence and Hybrid Information Technology, (ICCIT '08)*, 2008.

- 21) A. M. Sagheer, and N. Motter, "Complex public key cryptosystems" *Al Mansour journal* no.14, 2010.
- 22) N. Gura, A. Patel, A. Wander, H. Eberle, and S. Chang Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", *CHES*, August 2004.
- 23) M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Emergent properties: detection of the node-capture attack in mobile wireless sensor networks" In *WiSec 2008*.
- 24) P. kumar and H. J. Lee," Security Issues in health care applications using wireless medical sensors networks: a survey", *Sensor*, pp. 55-91, 22 Dec 2011.
- 25) G. H. Zang, C. H. Y. Poon and Y. T. Zang, "A Review on Body Area Networks Security for Healthcare", *International Scholarly Research Network ISRN Communications and Networking*, 2011.
- 26) Z. Mehmood, Nizamuddin, S. A. Ch, W. Nasar, and A. Ghani, "An Efficient Key Agreement with Rekeying for Secured Body Sensor Networks" *IEEE* 2012.
- 27) J. Wu, and D. R. Stinson, "Three Improved Algorithms for Multipath Key Establishment in Sensor Networks Using Protocols for Secure Message Transmission" *IEEE Transaction on Dependable and Secure Computing*, VOL. 8, NO. 6, November/December 2011.
- 28) N. Raveendranathan, S. Galzarano, V. Loseu, R. Gravina, R. Giannantonio, M. Sgroi, R. Jafari, and G. Fortino, "From Modeling to Implementation of Virtual Sensors in Body Sensor Networks" *IEEE SENSORS JOURNAL*, VOL. 12, NO. 3, MARCH 2012.
- 29) M. Majidi, R. Mobarhan, A. H. Hardoroudi, A. S. H-Ismail, and A. K. Parchinaki , "Energy Cost Analyses of key Management Techniques for Secure Patient Monitoring in WSN" 2011 *IEEE Conference on Open Systems (ICOS2011)*, September 25 - 28, 2011, Langkawi, Malaysia.
- 30) C. Marghescu, M. Pantazica, A. Brodeala, and P. Svasta, "Simulation of a Wireless Sensor Network Using OPNET" *IEEE 17 the International Symposium for Design and Technology in Electronic Packaging (SIITME)* 20-23 Oct 2011, Romania.
- 31) N. U. Amin, M. Asad, Nizamuddin, and S. A. Chaudhry, " An Authenticated Key Agreement with Rekeying for Secure Body Sensor Networks Based on Hybrid Cryptography " *International conference on Networking, Sensing and Control (ICNSC)*, pp.118-121, April 2012.

- 32) X. Wang, X. Wang and J. Zhao, "Impact of Mobility and Heterogeneity on Coverage and Energy Consumption in Wireless Sensor Networks," in Proc. of IEEE ICDCS 2011, Minneapolis, USA, June 21-24, 2011.
- 33) <http://Senseonics.com/news/first-implantable-continuous-glucose-sensor-to-achieve-high-accuracy-performance-in-people-with-diabetes>.
- 34) Y. Hoi-Jun, S. Seong, C. Namjun, and K. Hye "Low energy on-body communication for BSN". In: 4th international workshop on wearable and implantable body sensor networks (BSN 2007), Aachen, In IFMBE proceedings vol. 13. Springer, Berlin Heidelberg New York, pp 15-20.