A

Thesis Report

On

WIRELESS SENSOR NETWORK SECURITY USING CERTIFICATELESS CRYPTOGRAPHY

Submitted towards the fulfilment of requirement for the award of degree of

Master of Engineering

In

Wireless Communication

Submitted by:

Mishika Gill

Roll No: 801463014

Under the Guidance of:

Dr. Ajay Kakkar

Assistant Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

(Established under the section 3 of UGC Act, 1956)

PATIALA – 147004 (PUNJAB)

CERTIFICATE

Certified that the thesis entitled ***"wireless sensor network security using certificateless cryptography"*** being submitted by **Ms. Mishika Gill** to the **Department of Electronics and Communication Engineering, Thapar University, Patiala** in the fulfilment of the requirements for the award of the degree of **"Master of Engineering"** is a record of bonafide research work carried out by her. She has worked under my guidance and supervision and fulfilled the requirements for the submission of this thesis which has reached the requisite standard. The matter presented in this thesis does not incorporate any material previously published or written by any other person except where due reference is made in the text.

The results contained in this thesis have not been submitted in part or full to any other institute or university for the award of degree or diploma.

Dr. Ajay Kakkar
Assistant Professor,
Department of ECE,
Thapar University,
Patiala (P.B) – 147004
India

DECLARATION

I hereby declare that the report entitled **"wireless sensor network security using certificateless cryptography"** is an authentic record of my study carried out as requirement for the award of degree of ME (Wireless Communication) at Thapar University, Patiala, under the supervision of **Dr. Ajay Kakkar**, "Electronics and Communication Engineering Department" during masters course of engineering in wireless communications.

Date: 15 July, 2016

Mishika Gill

Roll No-801463014

It is certified that the above statement made by the student is correct to the best of my knowledge and belief.

Date: 15/7/16

Dr. Ajay Kakkar
Assistant Professor, ECED

Countersigned by:

Dr.Sanjay Sharma

Professor and head,ECED

Thapar University, Patiala

Date:

Dr.S.S Bhatia

Dean of Academic affairs

Thapar University Patiala

Date:

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr. Ajay Kakkar**, **Assistant Professor,** Electronics and Communication Engineering Department, Thapar University Patiala for his patient guidance and support throughout this report. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable. I am also thankful to our Head of Department, **Prof. Dr. Sanjay Sharma** , P.G. Co-ordinator **Dr. Amit Kumar Kohli** and branch co-ordinator **Dr. Hem Dutt Joshi**. I would like to thank the entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Mishika Gill
ME-WC
801463014

TABLE OF CONTENTS

Abstract

Secured and timely transmission of data is always an important aspect for an organization. In the encryption process the failure rate of keys and processing time are directly related with the security of cryptographic model in Wireless Sensor Network (WSN). The use of strong encryption algorithms almost make it impossible for a hacker to get access of node which is being protected by keys. Data security is an essential component of an organization in order to keep the information safe from various competitors. Current aspects of cryptography and need of data security in communication are discussed in the beginning of this thesis. It also covers the various key authentication techniques employed for the data security with their merits and demerits. The work done by the various researchers in the field of cryptography has also been discussed. Observations from literature survey, problem formulation, objectives and research mythology has been formulated to design a new methodology. Then a certificateless cryptographic scheme has been proposed that meets the objectives such as key uniqueness and secure communication. After presenting the proposed schemes, their results and comparison with existing schemes and among each other has been drawn. Finally, conclusions and the future scope of the proposed work have been mentioned.

List of Abbreviations

AODV	Adhoc On Demand Distance Vector
AES	Advance Encryption Standard
AKA	Authorization and key authentication
CA	Certificate Authority
CCA	Chosen ciphertext attacks
CLC	Certificateless cryptography
DES	Data Encryption Standard
DOS	Denial of Service
GPS	Global Positioning System
IBC	Identity Based Cryptosystem
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
PKC	Public Key Cryptography
WSN	Wireless Sensor Networks

List of Figures

LIST OF TABLES

CHAPTER 1

INTRODUCTION

This chapter throws light on the concept of wireless sensor network security and its terminology. It is a technique used to secure the data in wireless communication which has to be transmitted between two parties. It is extended from traditional use of Diffie algorithm with Elliptic curve cryptography to new versions of key authentication mechanisms.

1.1 Wireless Sensor Network

In the current scenario of the rapid growth of computer processing power are increased unexpectedly, but the price and size of computers have greatly reduced that encourages much computer use. The latest technologies have made huge advances in computer time and also improve the use of computers in our daily activities. Wireless sensor networks have received a lot of attention recently because of their substantial applicability to improve our lives. They help us in extending our ability to accurately monitor, study and control objects and environments of different scales and conditions such as the human body, geological, habitats and security monitoring. According to figure 1.1 sensed data is delivered to the user. Suppose that the data is detected by the node a sensor within the sensing field. Since the radio transmission range for each sensor is short, A, at first, transmits the data to the neighboring node B. In this example detected, the data can be routed through the ABCDE-sink path. Since, sink is already connected to the Internet, it can provide data detected by the user directly from the sink. Sensor nodes in sensor networks can independently process and analyze the data detected in cooperation within the network so they can cut redundant data observed within a network and provide only the data necessary for the user by the wells. In addition, sensor networks can dynamically adapt its topology[7]. After deploying sensor nodes in a sensor field, independently, they are the neighboring nodes, and start to communicate with each other in various ways, normally by using multi-hop communications. In wireless communication and embedded micro-sensing technologies, advances encourage the use of sensor networks today in many environments to detect and monitor sensitive information. These environments include border protection, disaster

areas, areas related to health, and control of smart home and much more Sensors contribute to the production of electricity, and also used in the collection of solar energy WSN.

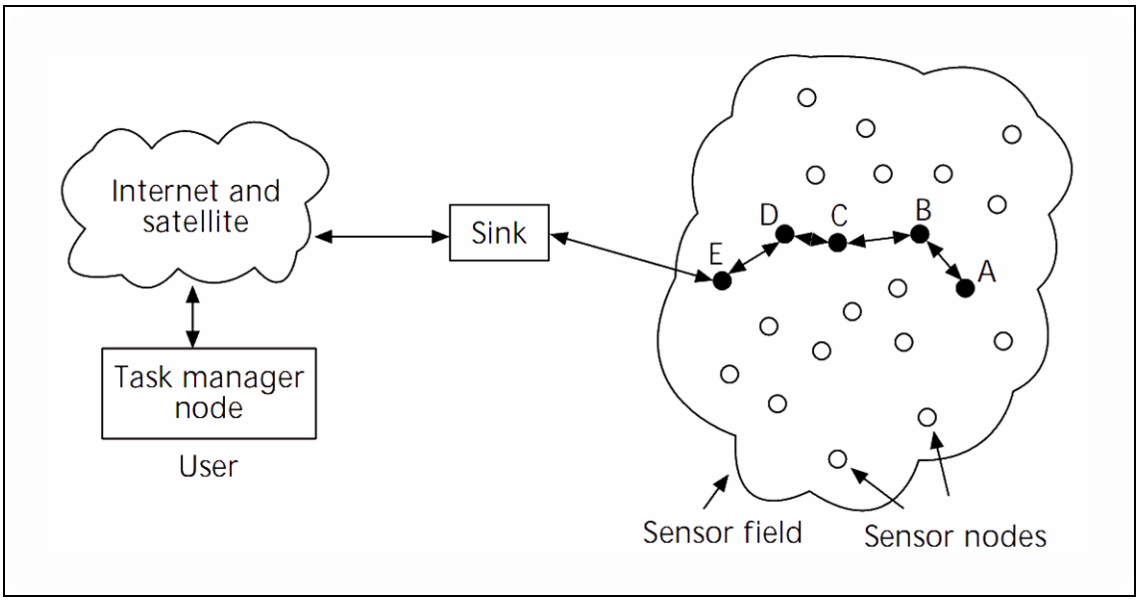

Figure 1.1 Sensor nodes scattered in a sensor field[7]

Now if sensor networks are becoming a reality in this world, but there are some limitations such as topology change randomly, restrictions in power, the limited computing resources such as energy, the environment errors , energy efficiency. Energy consumption is a major limitation of WSN which requires researcher's skills to get a way in reducing energy consumption by sensor nodes used in WSN.

In the latest research on WSN, researchers are trying to find and overcome the limitations of wireless sensor networks such as limited energy resources, ranging energy consumption by location, the high cost of transmission, and limited processing capabilities [25] All these characteristics of wireless sensor networks are totally opposed to their cable counterparts network, which energy consumption is not an issue, the cost of transmission is relatively cheap, and network nodes have a lot of processing power. [6] Routing approaches that have worked so well for traditional networks over twenty years will not be enough for this new generation networks.

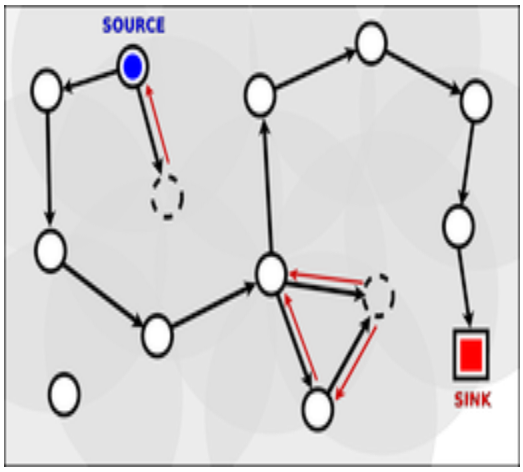

Figure 1.2 Representation of a network in which a node goes down due out of battery and a different path is chosen with a Single-path algorithm[54]

Besides maximizing the lifetime of sensor nodes, it is best to distribute the energy dissipated across the wireless sensor network to minimize maintenance and maximize overall system performance. [2] A communication protocol that involves synchronization between peer nodes incurs some overhead of setting up communication. WSN routing protocols or group to determine whether the benefits of more complex routing algorithms overshadow the additional control messages each node must communicate. [52, 3] Each node could make the most informed decision as to communications options if they had complete knowledge of the entire network topology and the levels of all the nodes in the supply network.

The usual topology of wireless sensor networks involves having many network nodes spread around in a specific physical area. [51] It is generally not architecture or specific hierarchy in place and therefore, wireless sensor networks are considered ad hoc networks. A network of ad hoc wireless sensors can operate in a standalone mode, or it can be connected to other networks, such as the largest Internet through a base station. [1] The base stations are generally more complex than simple network nodes and usually have indefinite power source. Regarding the limited power of the wireless sensor nodes of spatial reuse of wireless bandwidth, and the nature of radio communication cost that is a function of the distance squared transmitted, it is ideal to send information several smaller jumps than transmission over a long distance communication. [27] Generally, sensor networks clustering were of great interest. Grouping

nodes in clusters, leading to hierarchical routing and data collection protocols, was considered the most effective approach to support scalability in sensor networks[13]. The primary objective of most of the existing protocols lies on how to extend the lifetime of the network and how to make a more efficient use of critical resources, such as power butter. In addition, the combined need for rapid convergence time and minimum power consumption (in regard to the cluster formation process) leads to appropriate probabilistic (random or clearly hybrids) distributed clustering algorithms fast that soon became the most popular and widely used in the field.

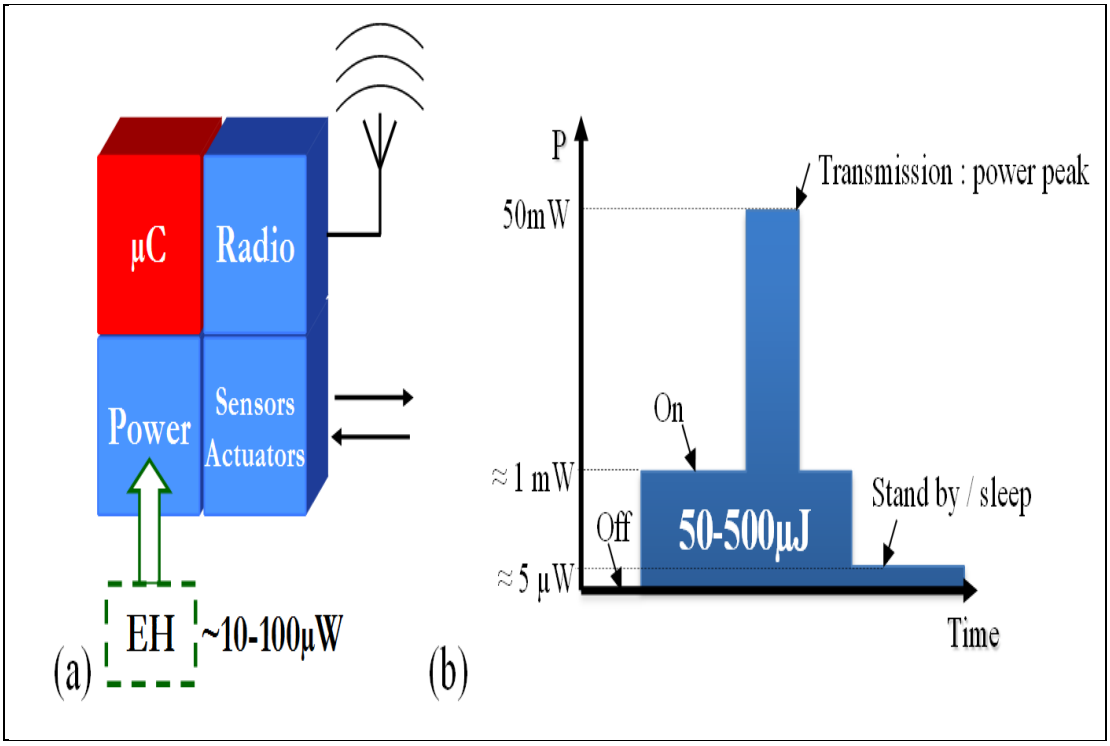

Figure 1.3: a) Autonomous WSN node and (b) sensor node's power consumption[23]

1.1.1 **Applications of WSN**

With new inventions in technology that allowed a sensor device to have higher cost performance and better as high resolution detection capabilities, observations over large areas for a number of detection devices became possible. Networking of these smart devices yet low-cost sensors to revolutionize the collection and processing of information in many situations.

- **Agriculture**: In agriculture, WSN is used to detect and monitor the condition of crops that promotes culture harvest lot by reducing their cost value cultivated crops also helps to improve the quality of crops.
- **Military applications**: In military WSN is used to detect and monitor the surrounding areas for any type of event. WSNs are there to detect and track tanks on a battlefield.
- **Forest fire detection**: Using WSN detects fires in a forest is another example where sensors are used to detect such fire events occur[10]. After detection sensor nodes, the BS reports to the location where the fire event occurred and then BS in response are some physical action such as sending the fire trucks are here immediately.

All these sensor networks characteristics are completely opposite to wired networks because in the cords of the energy consumption networks are not a problem. Unlike the applicability of various sensor networks, the battery capacity in their nodes is very limited, and it is unrealistic to replenish the battery nodes in many cases. Therefore, the preservation of this vital energy to each sensor node is significantly important in sensor networks.

1.1.2 Characteristics of WSN

The main features of sensor networks that play a vital role in the disintegration of their field of deployment such as detection and data processing, requires cheap hardware, nodes can easily fail, WSNs operate with strict energy constraints, WSN nodes have static nature, and the communication system is many to one rather than peer to peer.

1.1.3 Limitations of WSN

All these sensor network characteristics are completely opposite of cable networks where energy is not a matter of concern[11]. Energy is an important feature to increase the WSN sensor nodes lifetime to reduce maintenance costs and increase efficiency.

a) Limited Energy (energy consumption)
b) Network Life
c) Application Dependency
d) Secure Communication
e) Cluster formation and CH selection

f) Synchronization
g) Data aggregation
h) The repair mechanisms
i) Quality of Service (QoS)
j) Dynamic topology
k) Electric restrictions
l) The limited computational resources
m) Error-prone way to say wireless
n) Complexity
o) Lower speed than with the wired network
p) Security issues
q) Environment can affect network
r) Easily distracted with other technologies such as Bluetooth
s) The costly deployment of sensor nodes
t) Occurrence of the fault

1.2 Routing

Routing is the process which is the most essential part in the data communication networks to deliver packets from a source device to a destination device. In WSN, the three main routing categories are:

a) Flat-based routing: In this, all nodes perform equal roles and tasks.
b) Location-based routing: In this, all nodes data routing occurs according to their locations.
c) Hierarchical routing based: In this, all nodes have their own different roles of others.

1.3 General Sensor Network Architecture

The figure illustrates the general architecture of sensor networks:

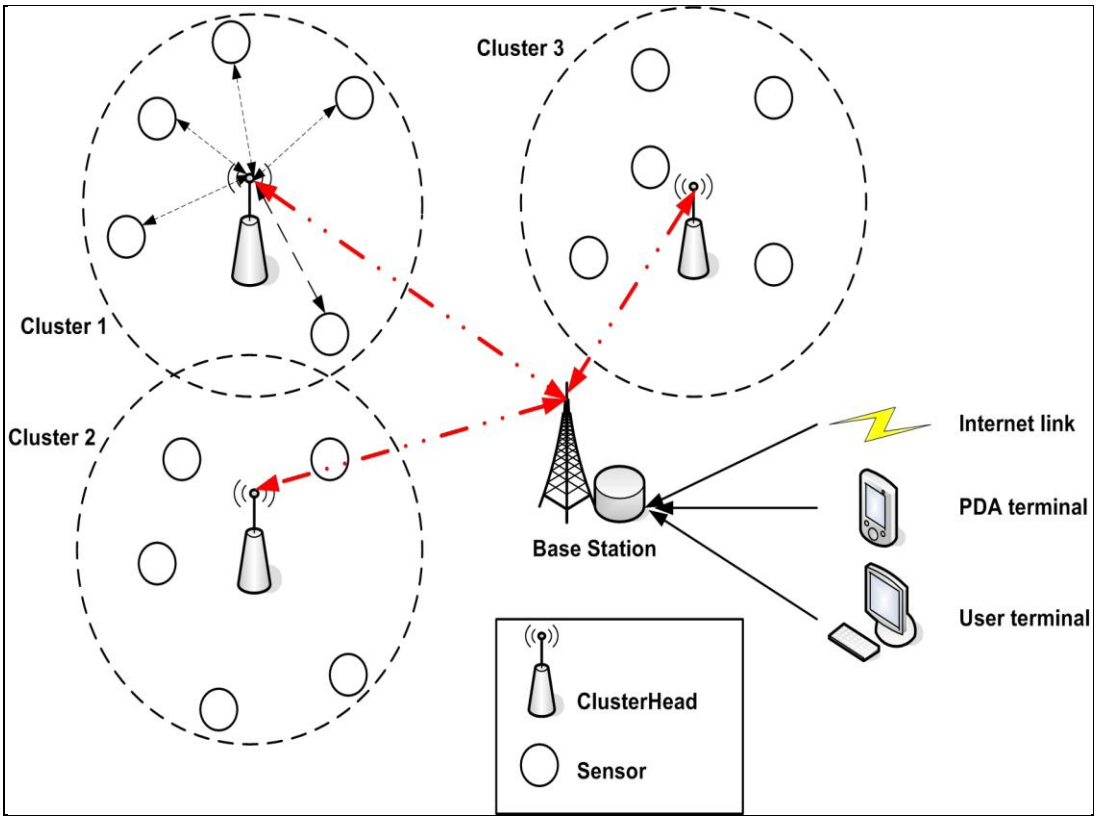

Figure 1.4: General Sensor Network Architecture[10]

- **Sensor Node**: sensor node is the major component of WSN because of its multi-role capabilities. It detects the data, stores data, routing data and processes the data.
- **Clusters**: Clusters are small, manageable units that simplify the tasks of such communication.
- **Cluster heads**: Chef's munitions are the leader who organizes the cluster functionalities. It grabs data from multiple sensor nodes, aggregates this data and arranges the schedule of a cluster for communication links to be established with BS.
- **Base station**: The base station is a central antenna element that collects data from multiple nodes in different locations. The deployment of the base station is also a critical issue of WSN. It acts as an intermediary between the network and the end user.

  The end user data in an array of sensors is used for a wide range of applications.

Therefore, a particular application may use the network data on the Internet, using a PDA, or a computer. In a network of sensors required (where the necessary data is collected from a

request sent by the network). This request is generated by the end user. Clustering phenomenon plays an important role not only in the organization of the network, but can significantly affect network performance.

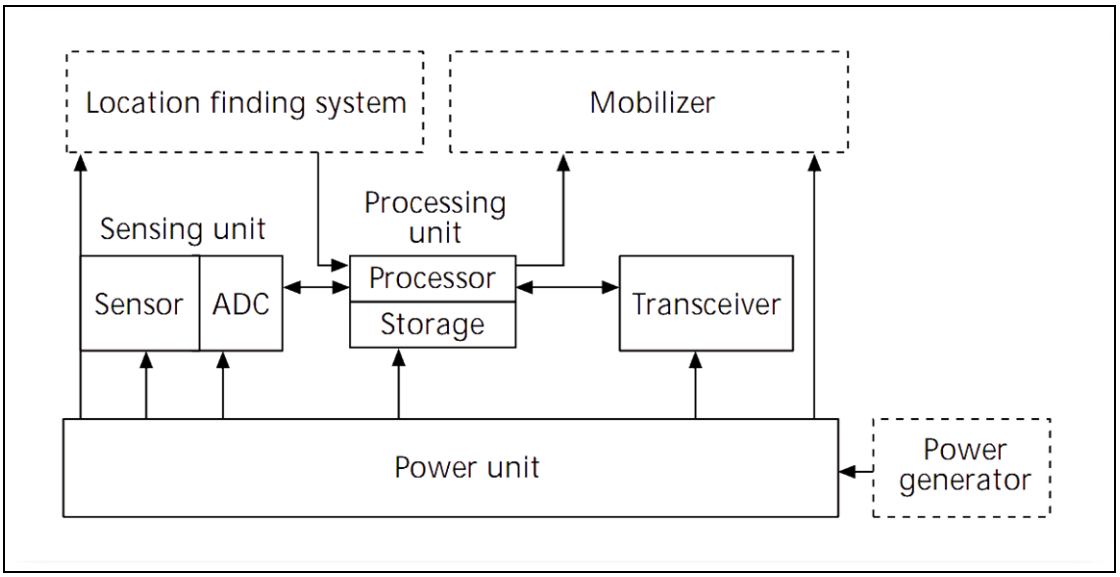

Figure 1.5: Components of sensor node[14]

1.3.1 Role of the sensor nodes in WSN

WSNs are deployed to collect information on areas for each event occurence. For this WSNs includes various sensor nodes that are used to monitor an area for events and after follow-up of these nodes relative to the BS (base station) about where the event took product. When BS receives event reports occurring ,it will reply with a quick physical message. In the sense-response applications, the sensor nodes are deployed in the coverage area overlapping with the detection area to prevent the holes. And more than one sensor nodes (nodes of neighbor) detects an event simultaneously and reports with BS and redundancy occurs[14]. In such a situation, the BS addresses this redundancy by responding only to those who are to come in the network domain. In this way, BS gets rid of false positives mean event that was reported to be never happened. Since the problem was solved, but what about the energy that is used in large quantities by each sensor node while the transmission of the event detected at the BS. Another solution would be for all neighbor sensor nodes reporting to a common node to say the head that transmit a message about an event detection BS and BS obtain the information detected by each node implicitly.

Various associated components forming a sensor node includes sensor, processor, storage and transceiver. Once the capture detection unit of an event comes in picture, it converts the analog signal into digital signal and transmits it to the processor as possible. Data can be stored in memory, and then transmitted to a node downstream of the sensor.

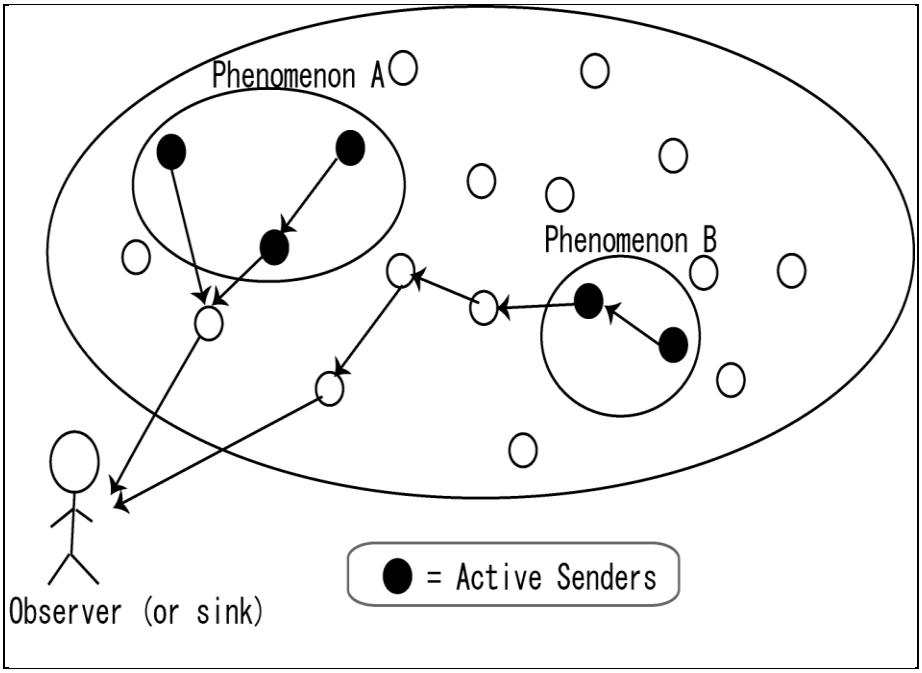

Figure 1.6: Intensive traffic from the fixed sets of nodes[42]

1.4 Need of security

The critical information shared over a WSN network needs to protect as it is subjected to threats and misbehavior of nodes [41]. Some of the general and essential security requirements are listed below:

a) **Data confidentiality**: information sensed by the node, mostly from the environment, need to be un-accessible and unreadable by the unauthorized neighbors. Public keys should also be in encrypted format so that sensor and key identities are protected from traffic as well as attacks.

b) **Data integrity**: ensuring that information being transmitted is not modified and altered

c) **Availability:** DOS attack which is very widespread and caused by the misbehavior nodes and overloading of node done by the intruder, need to be eliminated so that the

services provided by WSN are successfully delivered to each recipient and this is attained by a central access mechanism.

d) **Self organization**: self healing by a WSN is to be essentially accommodated as dynamic nature of WSN makes poses great threats to security.
e) **Time synchronization:** for group synchronization and multi hop applications, authorized users have synchronization protocols.
f) **Authentication:** message authentication code (MAC) computed from the secret shared key amongst the sender and receiver node to ensure the identities and also prevents injected fabrication of false nodes.

1.5 Security vulnerabilities in WSN

Mainly three types of attacks:

a) Attacks on network availability: DOS (denial of service) attack.
b) Attacks on secrecy and authentication: spoofing, packet replay attacks, eavesdropping, man in the middle attack.
c) Stealthy attack against service integrity; makes the network to incorporate a false data into the flow.

Organization of thesis

After going through the introductory aspects of sensors networks and the issues related to be taken under consideration. Thesis report is organized as , studying the research by various scholars worldwide on the same parameters or nearly relevant and the advancements throughout these years to tackle issues. After that we discuss the methodology proposed to cope with the security issues in key sharing mechanisms , focused on the parameters – entropy and resources involved to enhance the key uniqueness. Comparison is made with previous technique in fourth chapter with data tabulated.

CHAPTER 2

LITERATURE SURVEY

In this section we discuss the related work by various researchers worldwide and their proposed solutions that have been experimented so far to achieve dependability of WSNs taking into account intentional attacks as well as enhancing the different efficiency parameters of WSNs.

Jiguo li et al. [4] carried out cryptanalysis of two previous certificate based schemes(CBS) where there was no consideration of malicious Certificate Authority (CA) attack. CBS schemes without random oracles do not fulfill the unforgeability under the given attack. Thus, to withstand those attacks, author gives PKC-IBC scheme to achieve advantages in communication efficiency.

Sankardas roy et al. [5] worked on a large WSN, in network data aggregation significantly reduces the amount of communication overhead and energy consumption. The research community proposed a loss-resilient aggregation framework based on diffusion synopsis, which uses replacement of insensitive algorithms to accurately compute aggregates in multi path routing. They introduced the synopsis diffusion approach secure against attack over compromised nodes. In particular, they presented an algorithm to permit the base station to securely compute predicate count or sum even in the occurrence of such an attack.

Kia makki et al. [6] identified the threats to WSN and recapitulated the defense methods based on the networking protocol layer analysis. Then gave a holistic overview of security attacks enlisted. These issues are classified into seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other

security issues. Along the way they analyze the advantages and disadvantages of current secure schemes in each category.

Sanjay Keer et al. [8] developed a new protocol that prevents wormhole attacks over the wireless networks. It deploys the concept of asymmetric and symmetric key cryptography and Global Positioning System (GPS). It was evaluated using simulations under realistic ad-hoc network settings. The simulations acknowledged the strengths and weaknesses of this protocol under various distributions of GPS and non-GPS nodes.

Asad Amir Pirzada et al. [9] worked on Ad-hoc networks, which due to their offhand nature, are frequently installed under insecure environments, makes them susceptible to attacks. Ad-hoc on demand Distance Vector (AODV) is one of the widely used routing protocols that were currently undergoing extensive research and development. AODV is based on distance vector routing, but the updates are shared on an as per requirement basis rather than on a periodic basis.

Jjude H. Moore et al. [11] worked on sub-collection of keys with a palindrome sequence of round keys which are the weak keys, and those with anti-palindrome series of round keys, which are part of the semi-weak keys. The results offered help to identify the weaknesses of these keys.

A.Rajaram et al.[15] developed a trust based security protocol which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, they designed a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node was rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious.

Abdulhadi Shoufan et al.[16] presented a novel processor architecture for high-performance platform to carry out key generation, encryption, and decryption according to this cryptosystem. The McEliece public-key crypto employs NP-hard decoding, and hence is regarded as a way out for post quantum cryptography. Though early known, this cryptosystem was not engaged in as so

far because of efficiency issues regarding performance and communication overheads issue. A sample model of this processor was realized on a reconfigurable hardware and tested via a dedicated software interface. A comparison with a similar software solution highlights the performance advantage of the proposed hardware solution.

Razieh Mokhtarnameh et al [17] proposed security analysis that shows the key agreement protocol achieves almost all of the known desirable security attributes such as known key secrecy, key-compromise impersonation, unknown key-share, known session-specific temporary information security, forward secrecy and no key control. Furthermore, it conveys better efficiency in contrast to the existing protocols. In addition, the key generation and agreement protocols reduce the amount of trust on KGC. Currently, among the future work it includes reanalysing the efficiency of the proposed protocol in distributed environments, e.g. peer-to-peer and grid computing platforms.

Lin Zhu et al [18] worked on the key management problems of AMI systems, a novel KMS was proposed. From the security and performance analysis, the conclusion includes, a) The design of KMS is closely integrated with the three different transmission modes, which supports the unicast, broadcast, and multicast modes; b) the storage and computation of keys and related data are not a difficult task to be implemented in SMs or UGs; c) the distribution of the keys and related data will not affect the normal network traffic in an AMI system; and d) the KMS can deal with normal security problems; the forward and backward security can also be ensured.

Shandong Liu Nai-wen et al. [19] talked about data safety model in cloud computing. Firstly, it summarizes the cloud computing data application mode and gives data application system model in cloud computing system. Secondly, it evaluates the basic safety of cloud computing data platform. Cloud computing safety is not only a technical problem, but also involves other aspects such as standardization supervision model, laws and regulations by giving its model at the end.

Han-yu lin et al.[20] proposed a secure certificate-based three-party signcryption scheme which allows a signer to signcrypt a message for two selected recipients .they can independently decode

the ciphertext and then verify the signer's signature mark without cooperating with each other. It can be seen that the proposed scheme can be practically implemented, because either a signer or each of the two designated recipients only needs to perform one pairing computation for signcrypting a message or unsigncrypting a ciphertext. When repudiation occurs, each chosen recipient has the ability to reveal the signer's ordinary signature for public negotiation without compromising his private key. Compared with related mechanisms, earns more computational efficiency. Additionally, they also give security proofs of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery under adaptive chosen message.

Antonio Cortina Reyes et al.[21] provided an evaluation that could serve as a reference base for the scalar multiplication algorithm to meet the platform requirements such as memory or processing time in real time implementation of ECC-based cryptographic algorithm (encryption or digital signatures). As future work, algorithms for computing the scalar multiplication defined over other finite fields will be explored, as instance ($3m$).

It has long been held that errors in received noisy cipher texts need to be eliminated using possible powerful error correcting codes so as to reduce the avalanche effect on legitimate users' performance in block ciphered systems. The negative effect of erroneous ciphertexts on cryptanalysis by an eavesdropper were understood, nor the possible measurable trade-off between security enhancement and performance degradation under noisy ciphertexts. To address these questions, **Shuangqing Wei *et al.[22]*** launched a case study using Data Encryption Standard based block ciphers working in cipher feedback mode to show quantitatively the pros and cons of exploiting voluntarily or non-voluntarily introduced binary errors in ciphertexts of block ciphered systems using the proposed comparison metrics.

David Starobinski et al.[24] showed that the multichannel transceiving capability of sensors can be exploited to achieve significance reduction in the delay of data dissemination. In particular, judicious variations of round robin strategies can achieve near-optimal performance in important, practical topologies. Surprisingly, the presence of a separate radio (interface) for each channel is not needed to achieve substantial performance gain, proportional to the number of channels.

Finally they have shown that extreme value theory could prove functional in designing reliable data dissemination protocols with minimal control overhead.

Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. Recently, a random key predistribution scheme and its improvements have been proposed. A common assumption made by these random key predistribution schemes is that no deployment knowledge is available. Noticing that in many practical scenarios, certain deployment knowledge may be available a priori, they proposed a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. **Wenliang Du** et al.[25]showed that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can be substantially improved with the use of proposed scheme.

Meenakshi Sharma et al.[26] presented over the medium for sending and receiving the data between two parties i.e. Sender and receiver but communication needs the security from unauthorized people. It secures the network, as well as protecting and overseeing operations being done. For more security, they used Diffie – Hellman algorithm that is a specific method of exchanging cryptographic keys. The Diffie– Hellman key exchange method permits two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.In proposed work, they provided harder encryption with extend public key encryption protocol for security. It provided better end security implemented in any network.. The DH algorithm is improved by adding codes to the algorithm.

Maryam Ahmed et al.[27] The Diffie-Hellman key exchange exploits mathematical properties to fabricate a common computational result between two (or more) parties aiming to exchange information, without any of them providing all the necessary variables. By agreeing on two variables and providing each other with a computed public key, the resulting secret key will be identical throughout the exchange. It is, of course, possible to arbitrate by either hidden or by sheer brute force, but the former is a common concern — authentication — which must be addressed separately, and the second is computationally infeasible , the alternative name being exponential key exchange. This was achieved by prime generation, and true randomness in

picking variables, so as to make the D-H protocol can be a powerful component in many a security measure

M. Mehta et al. [28] worked on Diffie hellman that has been the most popular key agreement protocol for providing authentication to sign the result of a one –way hash function, based on cryptographic assumptions.This content studied the basics of the algorithm security based on discrete algorithm,elliptic curve and RSA .They have assessed the security on protocol level as a whole ,instead of considering algorithm level only.

Wang Houzhen et al.[30] identified mathematical Problem formulation of ergodic matrix and tensor product decomposition taking into consideration the computational complexity and algebraic structures, a new resistant quantum key exchange protocol was proposed so as to conveniently implement the matrix in both hardware and software and security bits made scalable.

Finite field operations have been in use so far in various applications ranging from error control coding to encryption computations.these computations include normal basis multiplications and exponentiations which are utilized in efficient applications due to their advantageous characteristics and the fact that squaring (and subsequent powering by two) of elements can be obtained without any hardware complexity. **Reza Azarderakhsh** et al.[31] presented 2-Dimensional decomposition systolic oriented algorithms to build up systolic structures for digit-level Gaussian normal basis multiplication and exponentiation over GF(2m). The given high-performance architectures are apt for a number of applications, e.g., architectures for elliptic curve Diffie–Hellman key agreement scheme in cryptography.Standards of efficiency, performance, and implementation metrics of such architectures through a 65-nm application-specific integrated circuit platform verify high performance algorithms for the multiplication and exponentiation architectures presented here suitable for high-speed architectures, including cryptographic applications.

Junghyun Nam et al.[32] worked on a session key which allows group communication in public networks with a common secret key. One such protocol is NEKED protocol proposed by

Byun et al. for password-authenticated group key exchange in mobile ad-hoc networks overseen by unmanned airborne vehicles .this plays a vital role in building secure multicast channels. Current work was about improving the security of the NEKED protocol as it was vulnerable to an attack against backward secrecy password security.

Vanesa Daza et al.[33] analysed an existing distributed key distribution scheme for low computational resources and servers based applications ,that are even paid in some way for doing most of the work.This explicit scheme achieved the preferred level of security in the random oracle model as long as the DDH problem is hard to solve. This was done by replacement of the protocol for the joint generation of a random value in [68] with a more secure one along with analysis of the security of a zero knowledge protocol, that provides robustness. A minor modification of the scheme in [68] which is also valid for the scheme in [69], replaces the use of a hash function with a table that must be managed by the servers. This results in less efficient key distribution schemes, maybe only suitable for scenarios where the expected number of conferences is small.

Horace p. Yuen et al.[34] explained the security issues in quantum key distribution (QKD), here focus was on issues related to cryptographic and information theoretic in nature and not those based on physics. The problem of security criteria was addressed. It showed that an attacker's success probabilities are the fundamental criteria of security that any theoretic security criterion must relate to in order to have operational significance. Trace distance errors were analysed in regards to 3 parameters: i.e. validity and accuracy of numerical security level. Complete quantitative description of the information theoretic security of classical key distribution is done. They had given a brief outline of the history of some major QKD security proofs, a rather hostile comparison of current QKD proven security with that of conventional symmetric key ciphers.

Shu-Di Bao et al.[35] focused primarily on the key distribution techniques with the EDPSs-based EIs for BSNs with healthcare solutions..A different approach based on AC/DCT was proposed aiming for a improvement in recognition rates. The randomness seen in the performance of EDPS-based EIs had proved that such EIs are with an acceptable level of randomness. The experimental analysis in terms of identification rate with the matching feature

number as the decision-making factor had been demonstrated that the EIs generated by the proposed schemes, that is, SWFT scheme and AC/DCT scheme, are more capable for securing of key materials, as of the existing MWFT scheme. Also an improved key distribution scheme, that is, user-dependent fuzzy vault, has been proposed to optimise the procedure of EDPS-based EIs. The on the whole performance analysis of authentication rate and computational complexity showed that the proposed solution can provide much higher success rates of key distribution with uncompromised security and less computational complexity compared with the existing one. It worked more effectively on upgrading the recognition rates for ECG.

Qiong Pu et al.[36] proposed an improved protocol called the cocktail-AKA protocol recently to beat the inherited discrepancies present in the UMTS's Authentication and Key Agreement (AKA) protocol standard.In this paper, they have shown that it has some security gaps, which can lead to an intruder to mount a denial of service attack and an impersonation attack. Finally, an effective countermeasure was suggested in the paper.

Teddy Furon et al.[37] Whereas the embedding distortion, the payload, and the robustness of digital watermarking schemes were well understood, the notion of security was still not completely well definite. The approach proposed in the last five years till now is too impractical and solely considers the embedding process, which is half of the watermarking scheme. This paper proposed a new measure of watermarking security, called the effective key length to capture the difficulty for the attacker to get access to the watermarking channel. This new methodology was supportive for additive spread spectrum schemes. Experimental protocols using either Monte Carlo simulations, region approximation, or rare event probability estimator allow better evaluation in this subject. For improved spread spectrum (ISS), analysis exhibited following improvements a) the robustness and the security of the scheme are better-quality to spread spectrum and b) estimating the secret keys from the observations only is not the best way to break the scheme. Moreover, a comparison with correlation aware spread spectrum (CASS) showed that ISS offers a better security than CASS for a given robustness.

Zhenfeng Zhang et al.[38]carried out a decentralized attribute-based encryption (ABE) approach, by creating a public key and issuing private keys to multiple users that reflect their

attributes without any alliance where any party can act as an ability is discussed. ABE scheme can remove much of the load during heavy communication and two-way computation in the setup phase of multi-authority ABE schemes, thus was preferred. Recently in IEEE Transactions Parallel Distributed Systems, Han et al. [3] initialised a motivating privacy-preserving decentralized key-policy ABE scheme, which was claimed to attain better privacy for users and provably secure in the standard model. However, after carefully revisiting the scheme, it brought to a close that their scheme could not resist the collusion attacks, hence failed to fulfill the basic security definitions of the ABE system.

Minkyu Kim et al.[39] did the cryptographic key generation and distribution scheme for the smart gird proposed by Xia and Wang vulnerabilityis discussed to the impersonation attack by which the adversary was able to impersonate the responder to the initiator. Furthermore, on the basis of this vulnerability, they pointed out that Xia and Wang's argument for resistance against the unknown key share (UKS) attack was incorrect.

Robert K. Cunningham et al. [40] studied the gap that arises in part due to an objective mismatch. The quality of a biometric identification is typically measured using false match rate (FMR) versus false nonmatch rate (FNMR). As a result, biometrics had been extensively optimized for this metric. However, this metric said little about the suitability of a biometric for key derivation. This article illustrated a metric that can be used to optimize biometrics for authentication. Using iris biometrics as an example,it explored possible directions for improving processing and representation according to this metric. Finally,it discussed why strong biometric authentication remains a challenging problem and propose some possible future directions for addressing these challenges.

Tolga M. Duman et al.[41] examined the secrecy rate enhancements that can be attained by applying CSI aided transmit signal design algorithms in SSK transmission.They had formulated and solved an optimal iterative algorithm along with two low complexity precoding algorithms. The results demonstrated that the proposed precoding schemes are capable of providing positive secrecy over a relatively wide range of SNR values.

Recently, Bertino et al. proposed a new time-bound key management scheme for broadcasting. **Chien-Ming Chen** et al.[47]claimed that as long as the three assumptions hold, their scheme was secure as it involved their scheme which was planted on the hardness breaking of elliptic curve discrete log problem, HMAC, and tamper-resistance devices. By means of security measures deployed, users cannot access resources that they are not granted to them, even if users collude.This scheme was insecure against the collusion attack and also had potential for some possible amendments to this scheme.

Jeng-Feng Weng et al.[48] enumerated the computational and storage costs of three different approaches for rekey generation in MBMS and demonstrate that without dynamic rekeying, the computational cost will increase rapidly when the number of users increases. It was not a feasible solution for a large scale network. Because 3G is a large scale network with huge bulk of users, it was therefore suggested that LKH with dynamic rekeying be deployed better in MBMS.

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to make a faster, smaller and more efficient cryptographic keys.**Dr. D.B. Ojha** et al.[49] gave a crystal clear scenario of a comparative study between ECC and RSA, ECC's advantages and some application of ECC like ECDSA. This demonstration included some of the theoretical and practical aspects of ECC.

Da-Zhi Sun et al.[50] studied significance of Elliptic Curves in Cryptography which formerly was independently established by Neal Koblitz and Victor Miller in 1985.Since then, Elliptic curve cryptography [ECC] had evolved as a immense field for public key cryptography (PKC) systems. In PKC system, use of separate keys to encode and decode the data was done. Since one of the keys is distributed publicly in PKC systems, the strength of security depends on large key size. The mathematical tribulations of prime factorization and discrete logarithm were earlier used in PKC systems. ECC has proved to provide same level of security with relatively small key sizes. The research in the field of ECC is mostly focused on its implementation on application specific systems. This kind of system had scarce resources like storage, processing speed and domain specific CPU architecture.

The above conducted literature survey motivates to design a scheme in the context of Internet Of Things where only authorized users can access the sensor network communication and holds access to query messages. This is very important part of preserving the privacy of users.

2.1 Observations

The study conducted over various parameters in ensuring security to the sensor networks, the main issue that need to be handled is enhancing the energy efficiency of the node. The critical analysis of the literature study leads further towards the finalization of the proposed solution, particularly towards the sensor network security with the stronger and flexible authentication scheme. Observations made in above survey relevant to key authentication are:

- elimination of certificates in PKC-IBC (public key -identity based cryptography)
- Hence ,elimination of key escrow problem.

2.2 Gaps in the study

Based on making further improvements in performance of key authentication in WSN security measures, it is intended to carry out further enhancement in this field of certificate less cryptography [CLC]. This could be achieved with lessening of the load of computational complexity at the node processor. A comparison on the entropy and resources involved in the authentication of key mechanism between the pair needs to be done.

2.3 Objective of Research

From the previous sections, objectives have been drawn and are as:

- To study the various encryption technices for data security.
- To analyze the various security protocols involved in key authentication process in WSN.
- To eliminate conventional key escrow problem in found in several protocols deployed for provoding security to key sharing mechanism in the variable networks.
- To compare the simulation results, based on the platform of enhancing key uniqueness and efficiency of the resources involved, given earlier in Identity Based Cryptography (IBC) with the proposed CLC-AKA

CHAPTER 3

METHODOLOGY OF THE PROPOSED WORK

The problem analysis of the existing schemes is conducted in order to construct the main problem formulation to carry on the thesis work over the enhancement of the wireless sensor network security. These methods incorporate enhancing the efficiency parameters of security measures studied so far for networks having link establishments based on adhoc communication.

Additionally, Elliptic curve Cryptography gives a brief overview of the developments that separate it from the traditional restrictions of wsn security using certificates. This evolved method allows misguiding the people who are not intended to view secret shares.

3.1. OVERVIEW OF THE PROPOSED TECHNIQUE

The existing model is based upon the certificate less cryptography identity-based cryptography (CLC-IBC) and has been improved for the higher efficiency among CLC-IBC. The CLC-IBC model has been comprised of the security model to protect against the information disclosure vulnerabilities and man in the middle attack. The existing system is two-column based key management authentication model with the elliptic curve cryptography. The existing model has been made to share four messages for one round of authentication. It utilizes the simple password exponential key exchange (SPEKE) model of the base model implementation and has been developed with certain defined improvements.

The proposed model is certificate-less cryptography authentication and key agreement (CLC-AKA). This model has been designed as the robust security architecture for the sensor networks. The proposed model is the authentication scheme for the sensor networks using the complex key models. The proposed model has been developed as the complex key architecture where the five columns based key model has been used for the secure authentication over the sensor networks. The equation driven mathematical programming has been incorporated for the purpose of key data generation over the node with the data origination. The receiver node propagates another set of the mathematical programming written to satisfy the procedure of key verification. The key

sharing method is supervised by the transmission module which circulates the key data between both of the nodes in the authentication pair.

3.2. STAGES FOR PROJECT IMPLEMENTATION

During very first stage the literature study is conducted over the authentication, key sharing, cryptography and several other domains to collect the information about the sensor networks, 3G/sensor networks, key sharing schemes, network architecture, etc

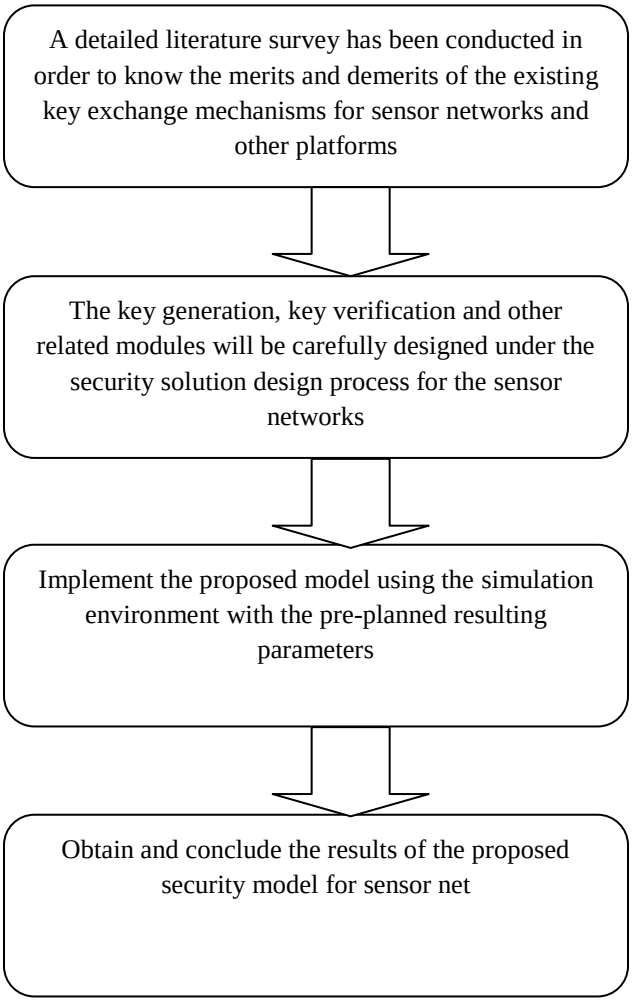

Figure 3.1: FPKA-SA methodology

The proposed model has been offered to protect the voice data and user data in the sensor network and environments. The key scheme has been designed to be used on the point-to-point architecture using the centralized base transceiver station (BTS) node. The base station ensures its security by using the authentication scheme between the sensor nodes and base station. The proposed model scheme has been enlisted as following:

3.3 Experimental Design

The design of the proposed solution has been prepared to mitigate the threats from the wireless sensor networks. The security of the pre-setup and post-setup phases has been covered under this system design by using the amalgamation of the cryptography methods along with the random generator key table production. The multi-column key pairing is utilized to scramble the key data up to the highly secure manner. The multi-round elliptic key cryptography has been utilized for the purpose of cryptography of the key data during transfers. The major aim of this thesis is to protect the sensor networks against the passive attacks which includes replication, replay and session hijacking attacks, which are launched to snoop the information from the active data channel.

For authentication purpose, we are using a table with 5 columns and multiple rows in which the first 3 columns (i.e. a, b, c) are used for query key generation and the last 2 columns (i.e. d, e) are used for reply key building. The table is shown below:

A	B	c	d	e

Table 3.1: Key Table

Query key generation

Query key= round(log10(sin(a)*cos(b)*tan(c))*887000+(a*b*c))

Reply key generation

Reply key= round(log10(sin(d), atan2(d,e)*180/pi)*347100)

3.4 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography to provide equivalent security. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks.

For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation

$$y^2 = x^3 + bx + c$$

along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.)

Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

3.5 Main Key Generation Policy:

Algorithm: Key Scheme Algorithm Sequence for Function Calling

CASE 1: When sensor initiates the data transmission to base station:

1. Sensor node initializes the setup phase, and request base station to complete the call.
2. The base station initializes the authentication process.

CASE 2: When the sensor initiates the data transmission to another sensor node:

1. The base station receives the setup call for the sensor node.
2. The base station requests the mobile station and verifies the ready state.
3. When sensor node replies with the ready state, base station initializes the authentication process.

MAIN ALGORITHM:

a) The base station infuses the multi-column keys to prepare the query key.
b) The query key is encrypted using the ECC algorithm.

c) The query key is forwarded to the mobile station.
d) The mobile station prepares the reply key by verifying the query key column data and marks the reply key rows.
e) The reply key is prepared by infusing the multiple keys information in the marked columns.
f) The reply key is encrypted using the ECC algorithm.
g) The reply key is forwarded towards the base station.
h) The base station verifies the query key against the reply and prepares the decision.
i) If the verification decision is successful
j) The call setup is complete and call is forwarded to the target mobile station.
k) Time counter (Tc) is initialized
l) Else
m) The call is dropped and the sensor node is informed about the authentication failure.
n) When the timer (Tc) expires, the exchange process is repeated.
o) If key verification is successful
p) The channel stays intact
q) Otherwise
r) The call is terminated

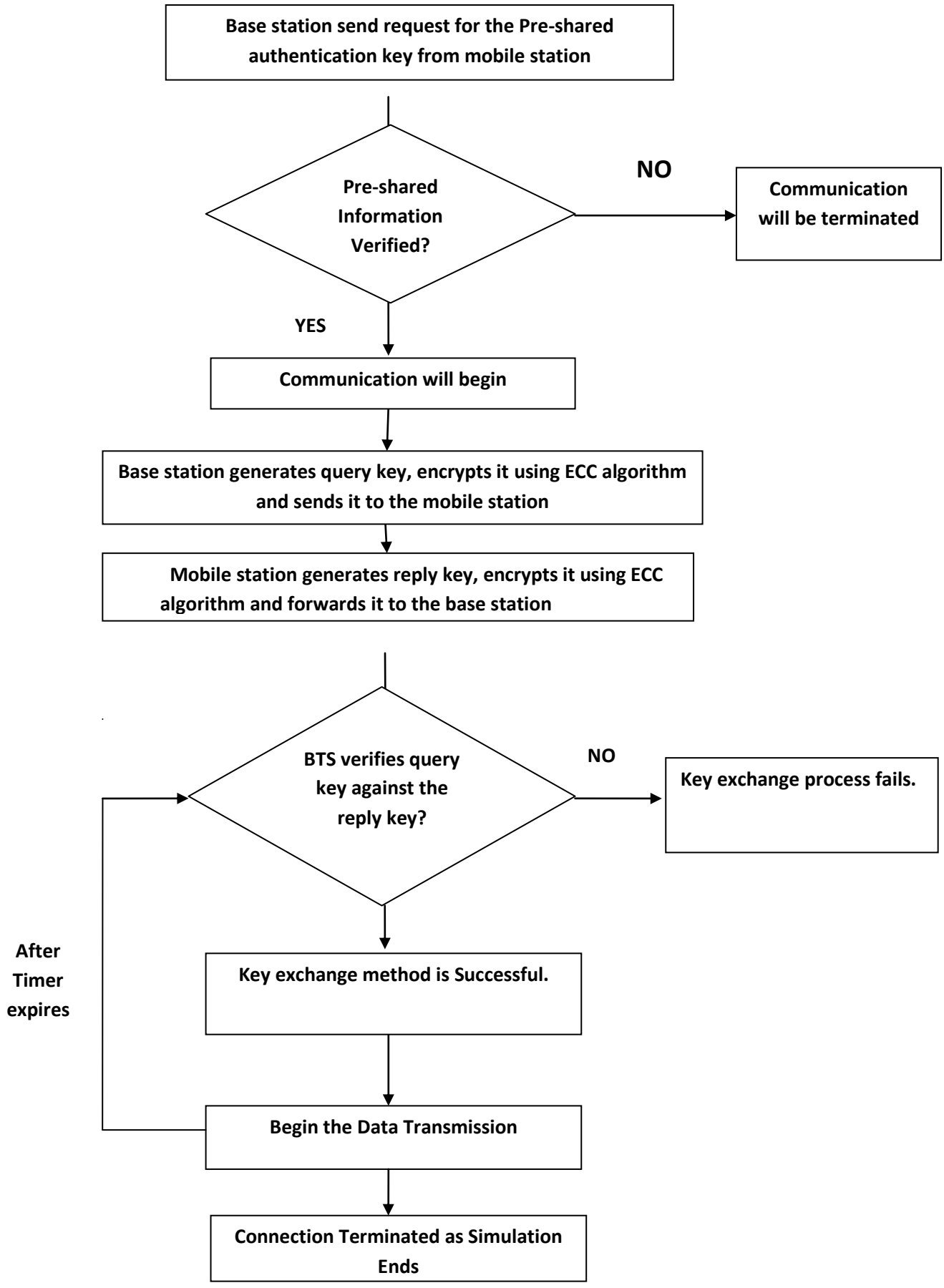

FIGURE 3.2: Proposed Key Exchange based Authentication Scheme Algorithm

CHAPTER 4: EXPERIMENTAL RESULTS

The efficiency of the proposed model has been evaluated for the voice data channelized over the sensor network channels for the simulation environment with unstable traffic and all the simulation has been carried out in the MATLAB.

4.1 Assumptions

Following are some pre-considerations regarding the communication channelization in the network with varying number of users (i.e population variation)

- Transmission delay due to traffic jam is zero.
- Channel assignment is automatic.
- Local processing delay is also assumed to be zero.
- BTS option: (Enable/ Disable)
- sensor nodes: (Enable/ Disable)
- Number of scenarios: 5
- Number of nodes: [1 5 10 20 50]

4.2 Results obtained from BTS

The results obtained from the proposed model simulation has been deeply analyzed and compared against the other schemes in order to evaluate the effectiveness of the proposed model.. The performance parameters of the projected resource and data overhead has been evaluated as the primary analysis factors which elaborates the performance of the proposed scheme in the terms of security and network performance. Also the size of the key population and its uniqueness has been tested with the entropy parameter. The results obtained for projected resources and entropy from the simulation of sensor network and BTS are given below.

Scenario 1: Scenario with 50 sensor nodes to the base station.

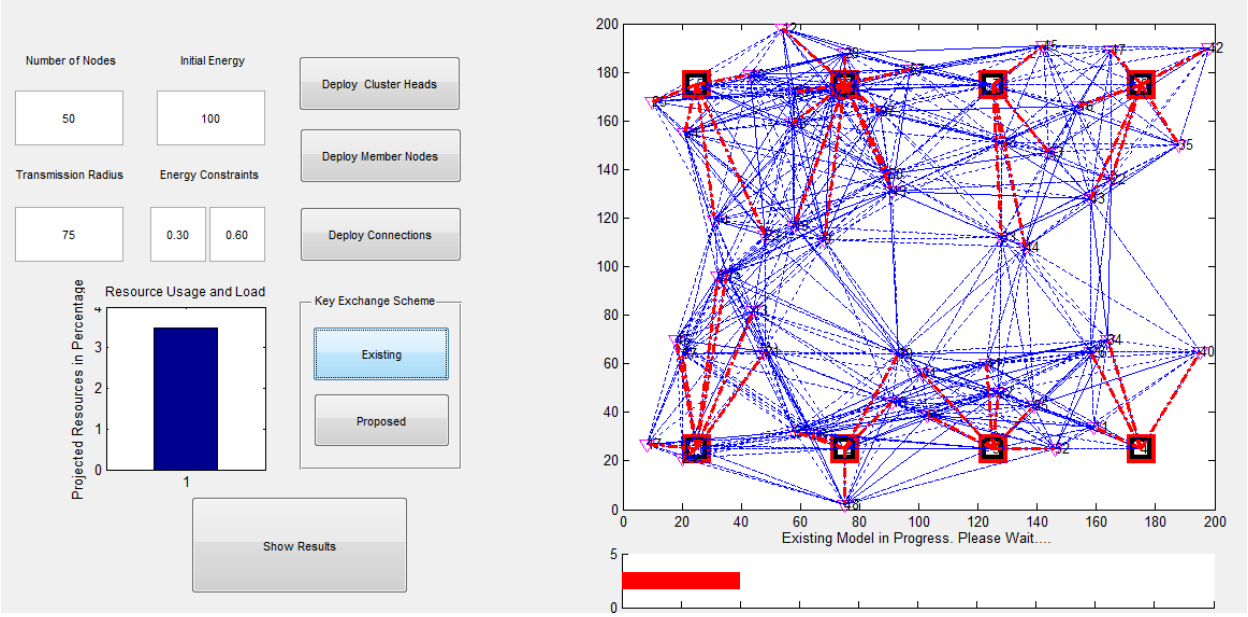

Figure 4.1: The system UI snapshot for Scenario 1

4.2.1 Results for scenario 1:

The projected resource has been evaluated for the measurement of the utilization of the resources over the given sensor network environment in the proposed model simulation. The high performance is indicated by the lower value of the projected resources computed from the simulation environment and higher value indicates the lower performance. CLC-AKA has been considered better than CLC-IBC as it has been measured with the lower value for projected resources over the given simulation scenario of sensor network. The detailed result evaluation has been described below:

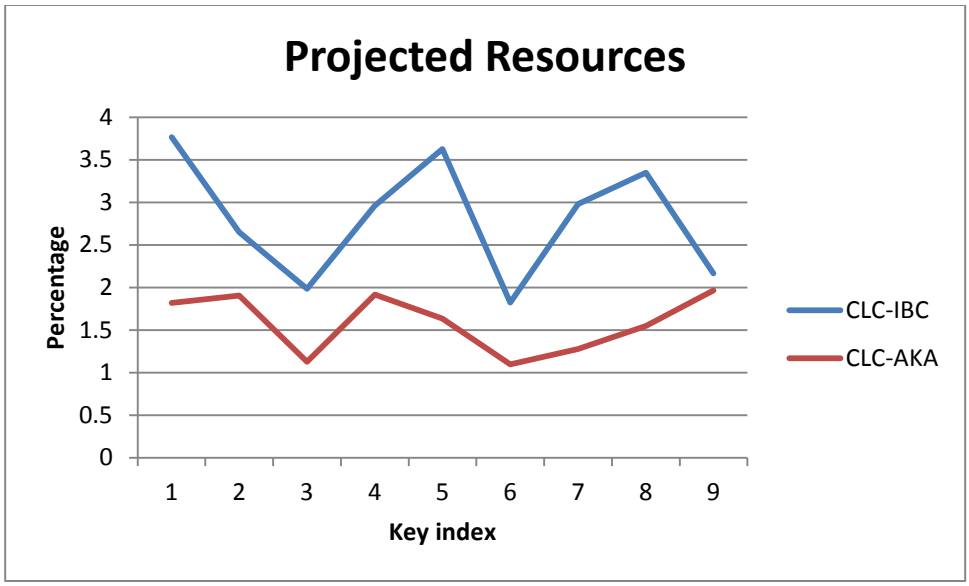

Figure 4.2: Projected resources based graph for scenario 1

The key efficiency, size of population and the uniqueness of the entities in the given key table is measured by using the entropy parameter. The unique data decreases the risk of key exposure to the hacking attempts, which has been strongly observed from the proposed model simulation. The consistently high entropy justifies the strength of the security of the sensor networks. The detailed results for entropy can be seen below:

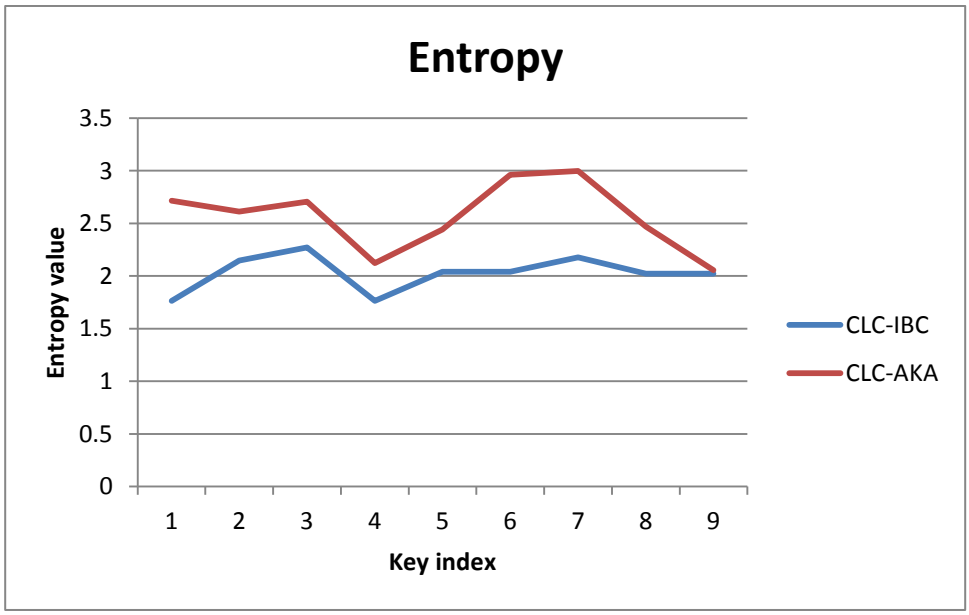

Figure 4.3: Entropy based graph for scenario 1

4.2.2 Comparative Analysis for scenario 1:

The comparison of the evaluated results has been performed over the results obtained from the existing and proposed models. The performance evaluation has been performed on the basis of projected resources and entropy. CLC-AKA has been proved itself as the better model than CLC-IBC. CLC-AKA has been proved to be efficient than CLC-IBC on the basis of both the performance parameters.

Key Index	CLC-IBC	CLC-AKA
1	3.7667	1.8164
2	2.6499	1.9063
3	1.9840	1.1250
4	2.9604	1.9141
5	3.6282	1.6328
6	1.8221	1.0977
7	2.9796	1.2773
8	3.3467	1.5469
9	2.1651	1.9648

Table 4.1: Projected Resources based comparison for scenario 1

Key Index	CLC-IBC	CLC-AKA
1	1.7632	2.7158
2	2.1466	2.6115
3	2.2706	2.7054
4	1.7632	2.1222
5	2.0412	2.4402
6	2.0412	2.9598
7	2.1762	2.9963
8	2.0207	2.4678
9	2.0207	2.0544

Table 4.2: Entropy based comparison for scenario 1

Scenario 2: Scenario with 100 sensor nodes to the base station.

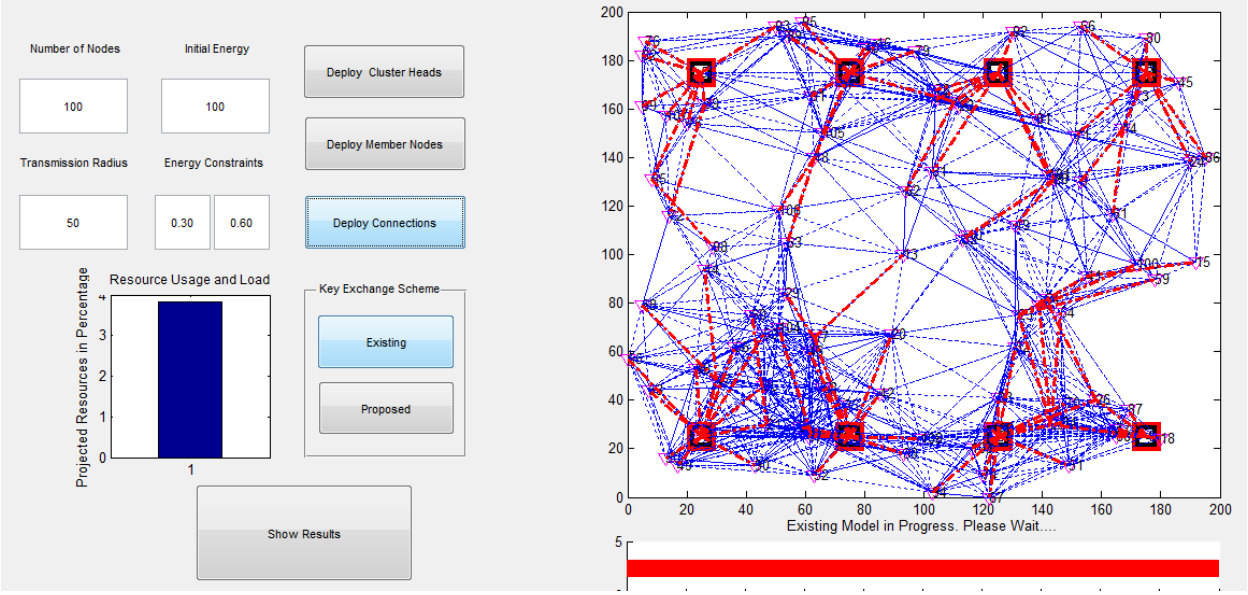

Figure 4.4: The system UI snapshot for scenario 2

4.3.1 Results for scenario 2:

The high performance in this scenario is indicated by the lower value of the projected resources computed from the simulation environment and higher value indicates the lower performance. CLC-AKA has been considered better than CLC-IBC as it has been measured with the lower value for projected resources over the given simulation scenario of sensor network.

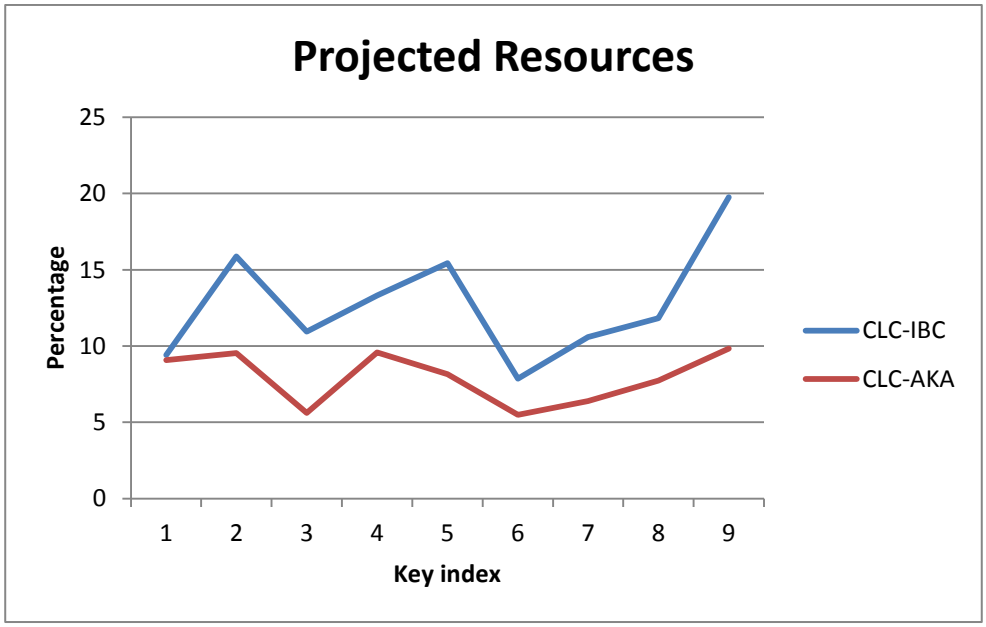

Figure 4.5: Projected resources based graph for scenario 2

The uniqueness observed from the obtained results has signified the decrease in the probability of the risk of key exposure to the hacking attempts, which has been strongly observed from the proposed model simulation. The consistently high entropy in the proposed comparison with existing model justifies the strength of the security of the sensor networks. The detailed results for entropy can be seen below:

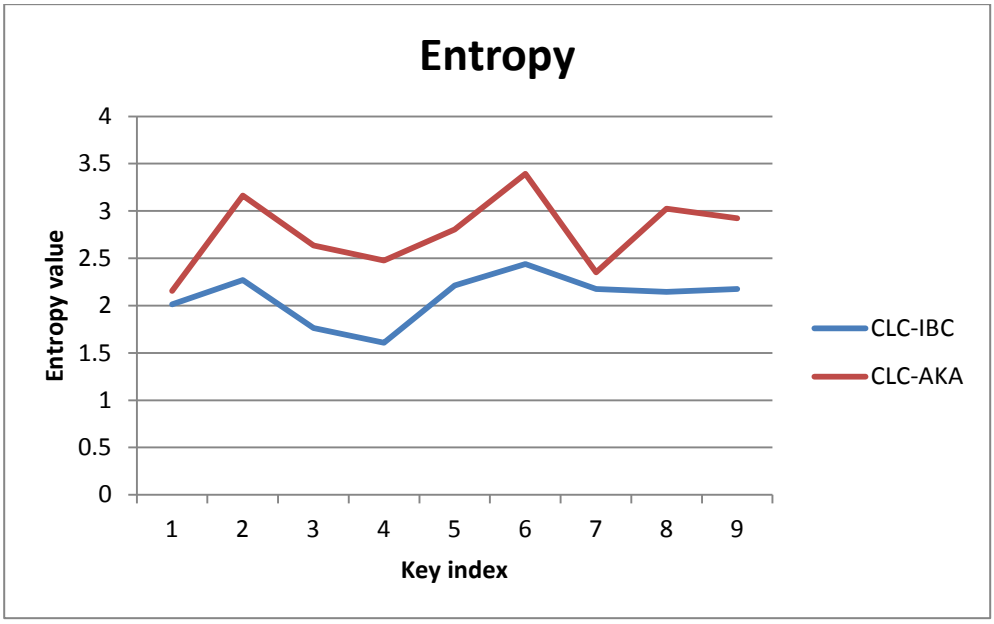

Figure 4.6: Entropy based graph for scenario 2

4.2.2 Comparative Analysis for scenario 2:

The comparison of the evaluated results has been performed over the results obtained from the existing and proposed model with five nodes. The performance evaluation has been performed on the basis of projected resources and entropy. CLC-AKA has been proved itself as the better model than CLC-IBC. CLC-AKA has been proved to be efficient than CLC-IBC on the basis of both the performance parameters.

Key Index	CLC-IBC	CLC-AKA
1	9.4108	9.0820
2	15.8686	9.5313
3	10.9425	5.6250
4	13.3108	9.5703
5	15.4245	8.1641
6	7.8656	5.4883
7	10.5811	6.3867
8	11.8138	7.7344
9	19.7488	9.8242

Table 4.3: Projected Resources based comparison for scenario 2

Key Index	CLC-IBC	CLC-AKA
1	2.0131	2.1550
2	2.2706	3.1638
3	1.7632	2.6344
4	1.6090	2.4772
5	2.2137	2.8043
6	2.4393	3.3921
7	2.1748	2.3524
8	2.1466	3.0257
9	2.1748	2.9228

Table 4.4: Entropy based comparison for scenario 2

Scenario 3: Scenario with 150 sensor nodes to the base station.

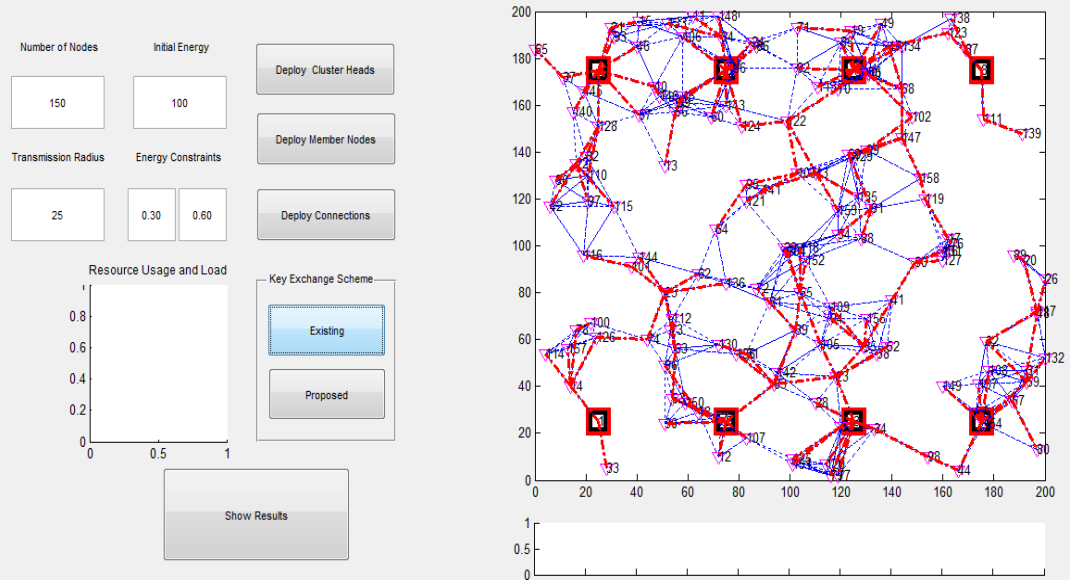

Figure 4.7: The system UI snapshot for scenario

4.4.1 Results for scenario 3:

The higher performance in the scenario with five nodes is indicated by the consistent lower value of the projected resources computed from the simulation environment and higher value indicates the lower performance. CLC-AKA has been considered better than CLC-IBC as it has been measured with the lower value for projected resources over the given simulation scenario of sensor network.

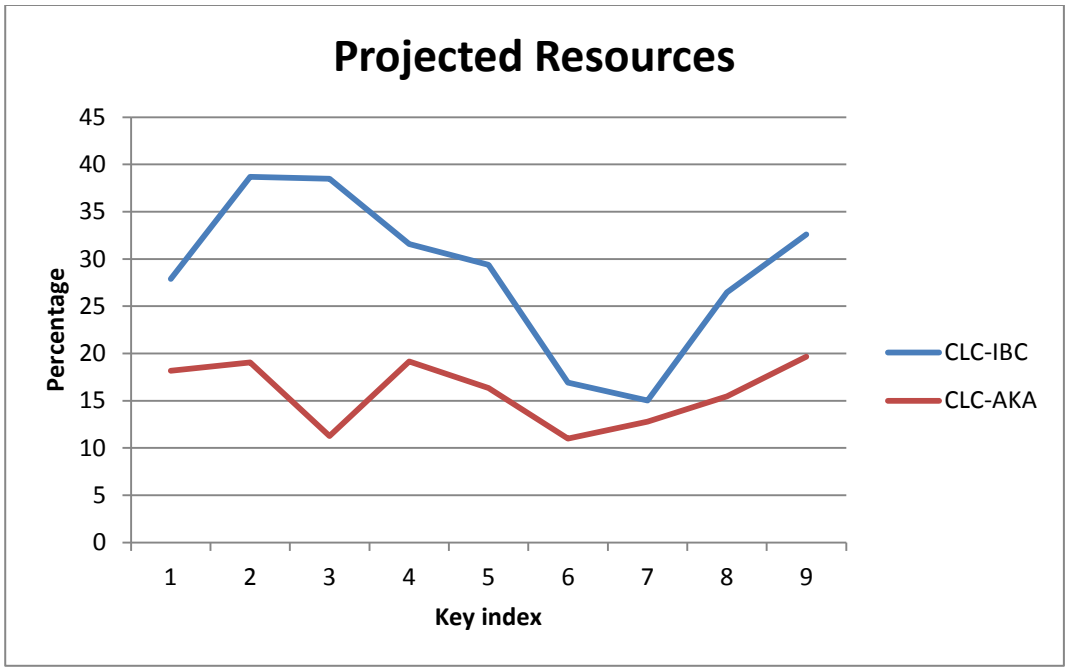

Figure 4.8: Projected resources based graph for scenario 3

The uniqueness observed from the obtained results has signified the decrease in the probability of the risk of key exposure to the hacking attempts, which has been strongly observed from the proposed model simulation. The consistently high entropy in the proposed in comparison with existing model justifies the strength of the security of the sensor networks.

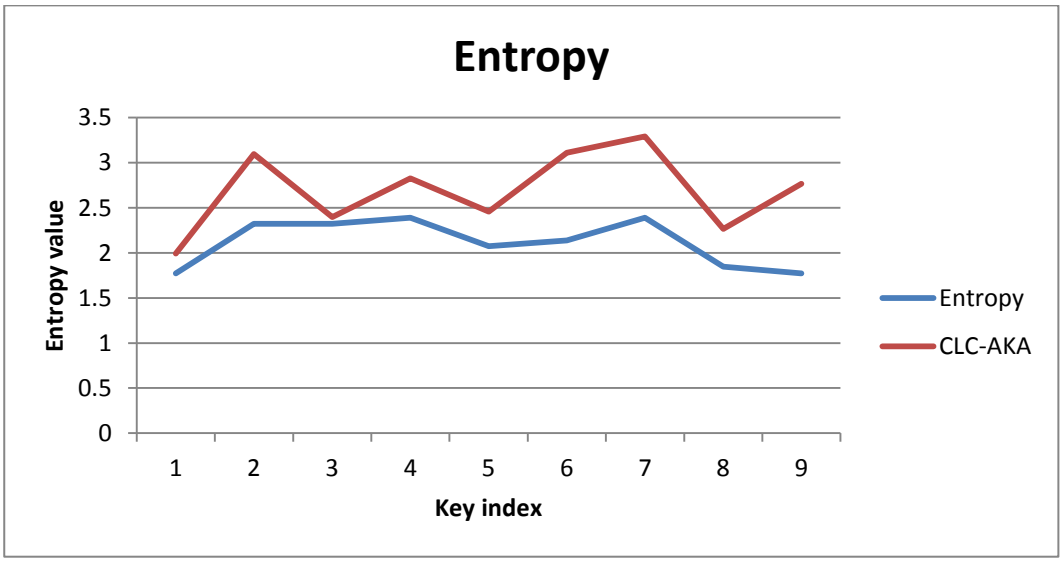

Figure 4.9: Entropy based graph for scenario 3

4.4.2 Comparative Analysis for scenario 3:

The performance evaluation over the ten number of nodes has been conducted on the basis of projected resources and entropy. CLC-AKA has been proved itself as the better model than CLC-IBC.

Key Index	CLC-IBC	CLC-AKA
1	27.8761	18.1641
2	38.6813	19.0625
3	38.4862	11.2500
4	31.5828	19.1406
5	29.3850	16.3281
6	16.9251	10.9766
7	15.0027	12.7734
8	26.4594	15.4688
9	32.5818	19.6484

Table 4.5: Projected Resources based comparison for scenario 3

Key Index	CLC-IBC	CLC-AKA
1	1.7707	1.9910
2	2.3225	3.0946
3	2.3225	2.3943
4	2.3884	2.8235
5	2.0712	2.4564
6	2.1370	3.1071
7	2.3884	3.2897
8	1.8462	2.2656
9	1.7707	2.7662

Table 4.6: Entropy based comparison for scenario 3

The following table (Table 4.7) indicates the robust performance of the proposed model.

Projected Resources	**S1:N50**		**S2:N100**		**S3:N150**	
	CLC-IBC	**CLC-AKA**	**CLC-IBC**	**CLC-AKA**	**CLC-IBC**	**CLC-AKA**
Average	2.6499	1.5469	13.3108	7.7344	26.4594	15.4688
Minimum	1.8221	1.0977	7.8656	5.4883	15.0027	11.2500
Maximum	3.7667	1.9648	19.7488	9.8242	38.6813	19.6484

Table 4.7: Projected Resources comparison between CLC-IBC and CLC-AKA

Additionally, the entropy parameter signifies the higher level of security in the CLC-AKA model than the existing model. The CLC-AKA model evaluation over the entropy has been described in the following table (Table 4.8).

The high uniqueness of the key table data increases the additional robustness to the security associated with the exchange of the keys between the sender and receiver nodes. The result of the proposed model has been observed nearly double than the existing model, which can be clearly indicated by the table 4.8:

ENTROPY	**S1:N50**		**S2:N100**		**S3:N150**	
	CLC-IBC	**CLC-AKA**	**CLC-IBC**	**CLC-AKA**	**CLC-IBC**	**CLC-AKA**
Average	2.0207	2.4678	2.0131	2.6344	2.0712	2.7662
Minimum	1.7632	2.0544	1.6090	2.1550	1.7707	1.9910
Maximum	2.2706	2.9963	2.4393	3.1638	2.3884	3.2897

Table 4.8: Entropy comparison between CLC-AKA and CLC-IBC

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

The proposed model named CLC-AKA has been compared against the existing model of CLC-IBC over the standard WSN simulation scenario with similar structure and environment. The detailed analysis of the simulation results has been conducted by analyzing the results obtained from the existing and proposed model simulations. The proposed model of CLC-AKA has been described efficient and effective while evaluated on the basis of the projected resources and entropy for the coalition of the network load and uniqueness respectively. Minimum of the 10 percent improvement has been observed in the favor of the proposed model when compared on the basis of various performance parameters in the variety of simulation scenarios. The attack situations have been analyzed theoretically and the effective in the results has been observed in the proposed model to mitigate the security threats with the new security model than the existing model. The new CLC-AKA scheme has been primarily evaluated for the utilization of the resources while using the security algorithm over the sensor network. The utilization of the resources, measured in the form of projected resources has been recorded significantly lower than existing model, which clearly indicates the robustness of the proposed model.

FUTURE WORK

The appropriate future enhancement of the proposed model may lies in the enhancement of the message level encryption for the insurance of the data security. The performance evaluation of the proposed model can be determined in the various aspects, scenarios and network platforms.

References

[1]R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, pp. 1,1978

[2]Diffie, W., and Hellman, M. New directions in cryptography. IEEE Trans. Inform. Theory IT-22, (Nov. 1976), 644-654.

[3] Dennis Gessner , Alban Hessler , Peter Langendoerfer “Application of wireless sensor networks in critical infrastructure protection: challenges and design options”, *IEEE Wireless Communications* Vol:17 , Page(s):44 – 49 Issue Date :October 2010

[4] Yang lu, Jiguo Li “Improved certificate-based signature scheme without random oracles”,research article *IET Journals Information Security*,pp. 1-7, june 2015.

[5] S. Roy, M. Conti, S. Setia and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", *IEEE Trans.Inform.Forensic Secur.*, vol. 9, no. 4, pp. 681-694, 2014.

[6] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor network security: a survey", *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52-73, 2009.

[7] V. Boyko, P. MacKenzie, and S. Patel. Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman (full version). http://www.bell-labs.com/user/philmac/research/pak.ps.gz

[8] Sanjay Keer, Anil Suryavanshi,” To Prevent Wormhole Attacks using Wireless Protocol in MANET”, *International Conference on Computer and Communication Technology,* 2010.

[9] A. Pirzada, A. Datta and C. McDonald, "Incorporating trust and reputation in the DSR protocol for dependable routing", *Computer Communications*, vol. 29, no. 15, pp. 2806-2821, 2006.

[10] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In CRYPTO’99, pages 537–554.

[11] J. Moore and G. Simmons, "Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys", *IEEE Transactions on Software Engineering*, vol. -13, no. 2, pp. 262-273, 1987.

[12] T. ElGamal. “A public key cryptosystem and a signature scheme based on discrete logarithm”, *IEEE Trans. Info. Theory*, 31:469–472, 1985.

[13] W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Info. Theory, 22(6):644–654, 1976.

[14] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In STOC’98, pages 209–218.

[15] A.Rajaram Anna University Coimbatore , Dr. S. Palaniswami “Malicious Node Detection System for Mobile Ad hoc Networks” (IJCSIT) *International Journal of Computer Science and Information Technologies,* Vol. 1 2010, 77-85 .

[16] A. Shoufan, T. Wink, H. Molter, S. Huss and E. Kohnert, "A Novel Cryptoprocessor Architecture for the McEliece Public-Key Cryptosystem", *IEEE Transactions on Computers*, vol.59, no. 11, pp. 1533-1546, 2010.

[17] R. Mokhtarnameh, N. Muthuvelu, S. Ho and I. Chai, "A Comparison Study on Key Exchange-Authentication protocol", *International Journal of Computer Applications*, vol. 7, no. 5, pp. 5-11, 2010.

[18] N. Liu, J. Chen, L. Zhu, J. Zhang and Y. He, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid", *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746-4756, 2013.

[19] P. Li, X. Chen, G. Zhang, B. Zhang and D. Huang, "An Advanced Commercial Contact Center Based on Cloud Computing", *IJIET*, pp. 407-411, 2012.

[20] H. Lin, T. Wu, S. Huang and Y. Yeh, "Efficient proxy signcryption scheme with provable CCA and CMA security", *Computers & Mathematics with Applications*, vol. 60, no. 7, pp. 1850-1858, 2010.

[21] Antonio Cortina Reyes and Ana Karina Vega Castillo “A Performance Comparison of Elliptic Curve Scalar Multiplication Algorithms on Smartphones”, *IEEE conference* pp.114-119, 2013.

[22] S. Wei, J. Wang, R. Yin and J. Yuan, "Trade-Off Between Security and Performance in Block Ciphered Systems With Erroneous Ciphertexts", *IEEE Trans.Inform.Forensic Secur.*, vol. 8, no. 4, pp. 636-645, 2013.

[23] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[24] D. Starobinski and Weiyao Xiao, "Asymptotically Optimal Data Dissemination in Multichannel Wireless Sensor Networks: Single Radios Suffice", *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp. 695-707, 2010.

[25] M. Boyarsky. Public-key cryptography and password protocols: The multi-user case. In ACM Security (CCS'99), pages 63–72.

[26] Rohini Er.Meenakshi Sharma CSE & Kurukshetra University, CSE & Kurukshetra University, "India Enhancing the Diffie-Hellman Algorithm". ACM Trans. Inform. Syst. Security, vol. 4, no. 3, pp. 275–288, Aug. 2001.

[27] S. Arora, "Resourceful Power Aware Routing Protocol in MANET", *International Journal Of Engineering And Computer Science*, 2015.

[28] L. Harn, W. Hsin and M. Mehta, "Authenticated Diffie–Hellman key agreement protocol using a single cryptographic assumption", *IEE Proc., Commun.*, vol. 152, no. 4, p. 404, 2005.

[29] Federal Information Processing Standards Publication, National Institute of Standards and Technology. Available: http://www. itl.nist.gov/fipspubs

[30] S. Mao, H. Zhang, W. Wu, J. Liu, S. Li and H. Wang, "A resistant quantum key exchange protocol and its corresponding encryption scheme", *China Communications*, vol. 11, no. 9, pp. 124-134, 2014.

[31] R. Azarderakhsh and M. Mozaffari-Kermani, "High-Performance Two-Dimensional Finite Field Multiplication and Exponentiation for Cryptographic Applications", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 10, pp. 1569-1576, 2015.

[32] Junghyun Nam, J. Paik, Ung Mo Kim and Dongho Won, "Security enhancement to a password-authenticated group key exchange protocol for mobile Ad-hoc networks", *IEEE Communications Letters*, vol. 12, no. 2, pp. 127-129, 2008.

[33] V. Daza, J. Herranz and G. S, "On the Computational Security of a Distributed Key Distribution Scheme", *IEEE Transactions on Computers*, vol. 57, no. 8, pp. 1087-1097, 2008.

[34] H. Yuen, "Security of Quantum Key Distribution", *IEEE Access*, vol. 4, pp. 724-749, 2016.

[35] F. Miao, S. Bao and Y. Li, "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security", *IET Information Security*, vol. 7, no. 2, pp. 87-96, 2013.

[36] S. Wu, Y. Zhu and Q. Pu, "Security analysis of a cocktail protocol with the authentication and key agreement on the UMTS", *IEEE Communications Letters*, vol. 14, no. 4, pp. 366-368, 2010.

[37] P. Bas and T. Furon, "A New Measure of Watermarking Security: The Effective Key Length", *IEEE Trans.Inform.Forensic Secur.*, vol. 8, no. 8, pp. 1306-1317, 2013.

[38] A. Ge, J. Zhang, R. Zhang, C. Ma and Z. Zhang, "Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme", *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2319-2321, 2013.

[39] Je Hong Park, Minkyu Kim and Daesung Kwon, "Security Weakness in the Smart Grid Key Distribution Scheme Proposed by Xia and Wang", *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1613-1614, 2013.

[40] G. Itkis, V. Chandar, B. Fuller, J. Campbell and R. Cunningham, "Iris Biometric Security Challenges and Possible Solutions: For your eyes only?Using the iris as a key", *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 42-53, 2015.

[41] S. Aghdam and T. Duman, "Physical Layer Security for Space Shift Keying Transmission With Precoding", *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 180-183, 2016.

[42] National Institute of Standards and Technology, Digital Signature Standard (DSS), "Federal Information Processing Standards Publication,"FIPS PUB 186-2, Reaffirmed, January 27, 2000.

[43] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Proc. Crypto '84, pp. 10–18.

[44] A. Arazi, "Integrating a key cryptosystem into the digital signature standard," Electron. Lett., vol. 29, no. 11, pp. 966–967, 1993.

[45] M. Naor, B. Pinkas, and O. Reingold, “Distributed PseudoRandom Functions and KDCs,” Proc. Int .Conf. Theory and Application of Cryptographic Techniques, pp. 327-346, 1999.

[46] Neal Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, vol.48:pp.203-209, 1987.

[47] Hung-Min Sun, King-Hang Wang and Chien-Ming Chen, "On the Security of an Efficient Time-Bound Hierarchical Key Management Scheme", *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 2, pp. 159-160, 2009.

[48]Jeng-Feng Weng, and Jyh-Cheng Chen”Dynamic Rekeying in 3GPP Multimedia Broadcast/Multicast Service”, *MBMSIEEE communications letters*, vol. 14, no. 4, april 2010

[49] K. Nyberg and R. A. Rueppel, “Weaknesses in some recent key agreement protocols,” *Electron. Lett*., vol. 30, no. 1, pp. 26–27, 1994.

[50] P. Zeng, K. Choo and D. Sun, "On the security of an enhanced novel access control protocol for wireless sensor networks", *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 566-569, 2010.

[51] R. M. Young, “Euler’s constant,” Math. Gazette, vol. 75, pp. 187–190, 1991.

[52] W. Feller, An Introduction to Probability Theory and Its Applications. John Wiley & Sons, Inc., 1957.

[53] M. Fogiel and J. R. Ogden, Handbook of Mathematical, Scientific, and Engineering Formulas, Tables, Functions, Graphs, Transforms. Research & Education Assoc., 1984.

[54] D. Bertsekas and J. N. Tsitsiklis, “An analysis of stochastic shortest path problems,” Mathematics of Operations Research, vol. 16, pp. 580–595, 1991.

final.docx

ORIGINALITY REPORT

20%	14%	18%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	mdpi.com Internet Source	2%
2	www.ncbi.nlm.nih.gov Internet Source	2%
3	research.cs.tamu.edu Internet Source	2%
4	www.mif.vu.lt Internet Source	1%