Secure Wireless Sensor Network Design Using aNew Method of High-Speed Lightweight Encryption

Prachi Kori
Department of Electronics and Telecommunication
Jabalpur Engineering CollegeJabalpur M.P
prachikoriv17@gmail.com

Dr. Kanchan Cecil
Department of Electronics and Telecommunication
Jabalpur Engineering College Jabalpur M.P
Cecil.kanchan@gmail.com

ABSTRACT

Information spilling over remote sensor organizations, where remote terminals (like PDAs, cell phones, and palmtops) access information conferencing frameworks, will achieve new difficulties. This paper aims to propose a high-speed lightweight encryption (HSLE) scheme for WSN controllers with low computational capabilities. This HSLE scheme reduces latency overhead by modifying existing methods to encrypt data using probabilistic data block encryption. The proposed work is also useful for protecting confidential data when it is transmitted via WSN or IOT; we simply need to save scrambled information on cloud servers. A brand-new key-based algorithm that substitutes HSLE encryption for high-end AES is being proposed.

With the same level of security, the proposed methods increase data encryption speed significantly; Additionally, they are ideal for hand-to-hand communication between mobile phones, palmtops, and other similar devices. algorithm can be used between sites where effective encryption is essential and processing power and battery power are limited. A wireless sensor network with no more than 100 nodes was built to test the proposed network node encryption system, and MATLAB is used to implement this work. In comparison to the other works that are currently available, the 100-node WSN's communication time delay is less noticeable.

The proposed work has accomplished most reduced encoding time among all suitable work and high BER than all suitable past works.

INTRODUCTION

1.1 INTRODUCTION

The digital revolution has benefited from modern communication's efficiency, speed, and cost-effectiveness; however, there are new threats to information and communication security. An XOR gate and a key can provide simple security because encryption is all about protecting our data from being interpreted by outsiders; However, a few simple transform techniques will soon make it clear. Techniques that are difficult to even recognize using transforms or other recursive mathematical solutions must be developed urgently. Size for data is a method that takes time and requires computation to encrypt full data. If we continue to do so, we will need to use several supercomputers to encrypt a full data file in real time. With different sorts of information and different information block rates, gatecrashers generally search with the expectation of complimentary information; Consequently, the level of security must be very high.

1.2 INTERNET OF THINGS

The term "Internet of Things," or IOT, is used to describe the billions of physical devices that are currently connected to the Internet and share and collect data. It is now possible to incorporate the Internet of Things into anything, from a pill to an airplane, thanks to the widespread availability of wireless networks and super-cheap computer chips. Devices that would not otherwise be able to communicate real-time data are given a new level of digital intelligence by connecting and adding sensors to all of these various objects. By bringing together the digital and physical worlds, the Internet of Things is making the fabric of the world around us smarter and more responsive.

1.3 MOTIVATION

Presently a days, most PCs and laptops have a couple of sorts of antivirus and individual firewall programming to forestall information burglary and furthermore on cloud servers. What happens, on the other hand, if other users on the same server gain access and steal confidential images or data? In 2006, a global study by market research firm Gartner found that while network intrusion and cloud servers are linked to 28% of information (data, audio, and data) theft, lost or stolen mobile devices may be responsible for 58% of data violations. In light of that, associations actually should reinforce assurance by encoding information, sound, and information no matter how you look at it. The significance of data security in the event of physical device loss is put into perspective by headlines from any newspaper, website, or news source worldwide. In the US (U.S.A.), the Transportation Security Organization (TSA) detailed that a PC robbery uncovered in excess of 100,000 individual records, including a few classified information. A laptop that contained personal information for 11,000 politicians was stolen from a ministry department in

Nottinghamshire in the United Kingdom (UK). Finally, the New Zealand Inland Revenue Department (IRD)'s asset audit in 2006 revealed that IRD has no HSLE regarding the whereabouts of 107 of its computers or the contents of those computers, which led to scandals. Encryption is necessary because the list is so extensive and long.

1.4 OBJECTIVE

We want to use an encryption method that doesn't necessarily use S-box, doesn't use slow memory, and can be done on WSN processors with limited computational powerto protect our data.

1.5 PROBLEM STATEMENT

Following issues are happen in past strategies –

- The proposed work utilizes Rapid Lightweight Encryption HSLE encryption method rather for k-n emit or RC4 and another recipe based information block informational index locater that depends on KEY, not type, for information.
- Proposed Fast Lightweight Encryption HSLE encryption is the most ideal according to the necessities and the proposed HSLE is prepared to do ongoing information encryption since it doesn't require a long investment to foster code information.

1.6 APPLICATIONS

- Web of Things (IOT)
- Observation and checking for security
- Danger identification
- The environmental
- Air pressure, humidity, and temperature
- The level of background noise
- Applications for medicine like monitoring patients
- Detection of Landslides and Agriculture

1.6 THESIS ORGANIZATION

Chapter 1 discusses the introduction, motivation, problem statement and objective of proposed work.

Chapter 2 discusses about the technologies and wireless sensor network.

Chapter 3 discusses available work and their outcomes. Literature has been taken from various

INTRODUCTION

WSN is a foundation less remote organization that is sent with an enormous number of remote sensors in an impromptu way that is utilized to screen the framework for physical or ecological circumstances. WSN uses sensor nodes and an onboard processor to manage and monitor a specific area's environment. They are connected to the base station, which is the WSN System's processing unit. A base Station in a WSN Framework is associated with the Web to share information.

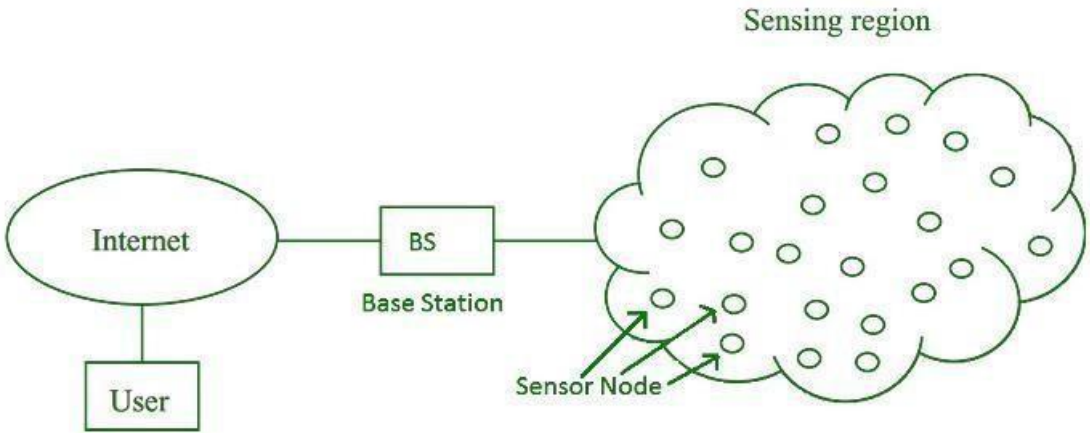


Figure 2.1 WSN can be used for processing, analysis, storage, and mining of the data [20]

2.1 Existing WSN Deployments

These days, there are a few genuine WSN situations utilized around the world. The main ones are portrayed. Sky blue Microsoft: WSN executed in Microsoft Azure is responsible for the effective administration.

Of the world's most famous administrations, like Ofice365, Skype, OneDrive, Xbox, and Bing search. Dissimilar to customary WSN organizations, Azure utilises different regulators for explicit applications. These regulators work in bunches and are

progressively constrained by local regulators. Correspondence between them is given using a northward API. On the sending plane, Azure is utilizing the OW tables like the ones characterized in OpenFlow. To streamline dormancy and execution of switches managing huge amounts of traffic, an extra layer was set up between sending gadgets and regulators. Microsoft included a virtual organization specialist for each hypervisor. This specialist is then reaching the regulator in the situation that no matching is found in the switch table. This arrangement moves the computational overhead from switches to all the more impressive host gadgets and permits more effective utilization of OS-level APIs for correspondence.

One of the main highlights of Azure's WSN is computerization. Assuming that any client characterizes its organization, strategies, and tendencies to plan using the web application, these progressions are naturally driven through regulators into the system administration gadgets. This will powerfully change geography.

B4 WAN Network, Google: Google's B4 WAN is probably the biggest organization of its sort on the Internet; associating 12 server farms spread all over the planet. This organization is utilized for information reflecting between server farms, file pushes, end-client information replication, and inside applications. B4 network has the accompanying elements:

- Brought together traffic design permits to improve on the organization's executives.
- Greatest connections use: common WAN connections are intended to be used at around 30 - 40% in normal, so if there should arise an occurrence of a connection disappointment, traffic sending isn't upset.

By dependably using connections at to around 100%, Google figured out how to decrease the expenses of these connections by up to 66%. Such a high usage, while guaranteeing unwavering quality, is made conceivable by utilizing multipath sending dependent on accessible connection limits. This is reachable because of the explicit prerequisites of Google's WAN applications, which can support worldly personal times or connection limit decreases. Then again, assuming a high limit is accessible, these applications can utilize it. Separated equipment and programming improves on arranged and impromptu organization changes and permits autonomous updates of servers and exchanging equipment. B4 is most likely the world's biggest WSN WAN in dynamic use. Since its creation, it has demonstrated its value and dependability with just one significant blackout, which was completely equivalent to the blackouts found in comparable WANs dependenton the customary system administration.

EC2: Amazon: According to EC2 (Elastic Compute Cloud 2-some portion of Amazon Web Services) utilizes WSN for mechanization, cloud development, security zones, versatile burden adjustment and network confinement. Robotization is significant for cloud administration as it permits dynamic and safe alteration of the organization's geography, expansion or expulsion of virtual servers, and so on. Network disconnection permits the utilization of covering IP addresses for various shoppers. Albeit Amazon isn't distributing insights regarding its WSN arrangement, it shows up that EC2 has utilized WSN beginning around 2013 (however likely considerably longer).

2.2 Components of WSN

Sensors: Sensors in WSN are utilized to catch natural factors and are additionally utilized for information procurement. Electrical signals are produced from sensor signals.

Nodes Radio: They are utilized to get the information created by the Sensors and send it to the WLAN passage. It has a power source, an external memory, a transceiver, and a microcontroller.

Access Point for WLAN: It takes in the data that radio nodes send wirelessly, typically via the internet, to it.Software for Evaluation: A piece of software known as Evaluation Software processes the data that is received by the WLAN Access Point in order to provide users with a report on the data's processing, analysis, storage, and mining.

2.3 SOFTWARE-DEFINED NETWORKING

SDN is an advanced worldview for PC organizations. SDN cuts the solid design of gadgets from the customary IP organization into two layers: sending and control. The sensing layer is lefton a system's administration gadget, where it utilizes existing information structures for bundle dealing. The control layer, then again, is moved to a different and concentrated gadget called an SDN regulator. The regulator oversees sending rationale inside the entire organization. Layer partition and control centralization permit the dynamic programmability of any organization's usefulness. This would be generally unimaginable in customary system administration gadgets, which have fixed highlights dependent on seller support. SDN is an innovation encountering a powerful development, and it is as of now at the focal point of consideration in the systems administration research area. SDN is investigated from many perspectives, and SDN organizations in different fields are thought of. SDN observed its pertinence, especially in server farm organizations. Driving organizations like Google, Amazon, or Microsoft have been effectively utilizing SDN in their organizations for a long time. Utilization of SDN in this climate assists with decreasing framework costs and permits full use of the current geography and use of cutting-edge highlights (like savvy load-adjusting, or quick failover systems). These days, SDN is being applied in present-day ideas including IOT networks like brilliant urban areas. It is likewise expected, that SDN will turn into the fundamental structure block for future 5G organizations [2].

The most customary meaning of SDN depends on two premises: partition of the control plane and sending plane and consistent centralization of the organization control. This idea consequently cuts the customary engineering of systems administration gadgets and characterises a new systems administration reflection using an upward partition, as portrayed in Figure 2.1. The Partition of control and information planes permits the controlling rationale to be put on a dedicated gadget, the regulator, which can be effortlessly customized utilizing normal programming dialects like C++, Java, or Python. This permits a moderate difference in the organization conduct and guarantees future organization developments [6].

SDN, in its later idea, is considered a "structure with numerous answers for a bunch of issues" [7]. This definition shows the wide scope of regions, where SDN can be sent. Despite the SDN definition, the main elements of SDN are:

- Brought together control-the entire organization can be controlled from a solitaryspot,simplifying network the board and compelling.
- Advancement and development - new elements can be easily added to theorganization.
- The board screens and oversees assets of systems administration gadgets andavailability inside the entire organization.
- Programmability-design changes can be made rapidly and progressively.

SDN, in its later idea, is considered a "structure with numerous answers for a bunch of issues" [7].

SDN is a general innovation, and there are genuine questions concerning its development. How well can a programmable methodology adapt to the notable and demonstrated idea of conventional systems administration, which has existed for nearly 50 years? Could a conventional programming approach supplant exceptionally particular equipment gadgets? What does this methodology mean for execution? Also, shouldn't something be said about security? Additionally, how network programming ought to be composed is, in itself, a broad subject.

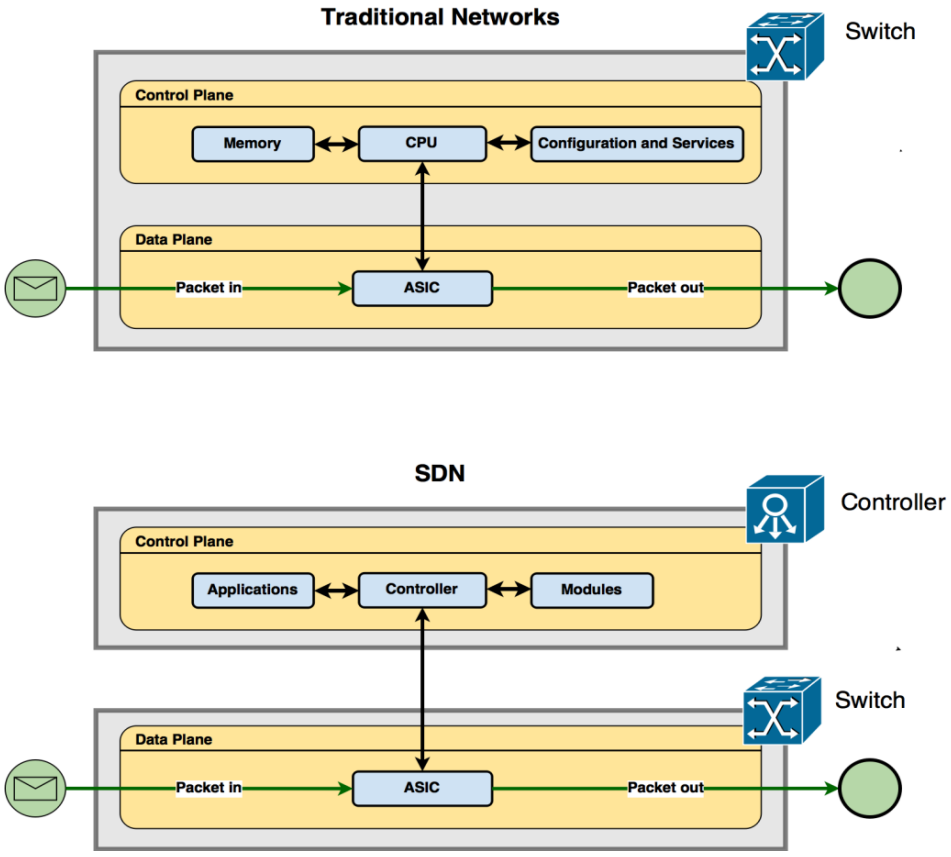


Figure 2.2: Traditional Networks and SDN [19]

It is clear that while offering many advantages, the SDN approach also has likewise numerous entanglements, including:

- Brought-together methodology - can deal with the whole organization successfully; however, it addresses a weak link. Assuming the regulator is assaulted, cut down, or simply needs a product update, the whole organization can become inaccessible.
- Conventional boxes: bring merchant freedom and a permit to join equipment discretionarily. Sadly, right now, the expense of these cases surpasses the expense of the comparatively well- prepared shut boxes of the customary system administration.
- Programmability: permits the composition any code with practically any conceivable usefulness. In any case, a gravely composed application can cut the SDN regulator down or permit a potential assault.

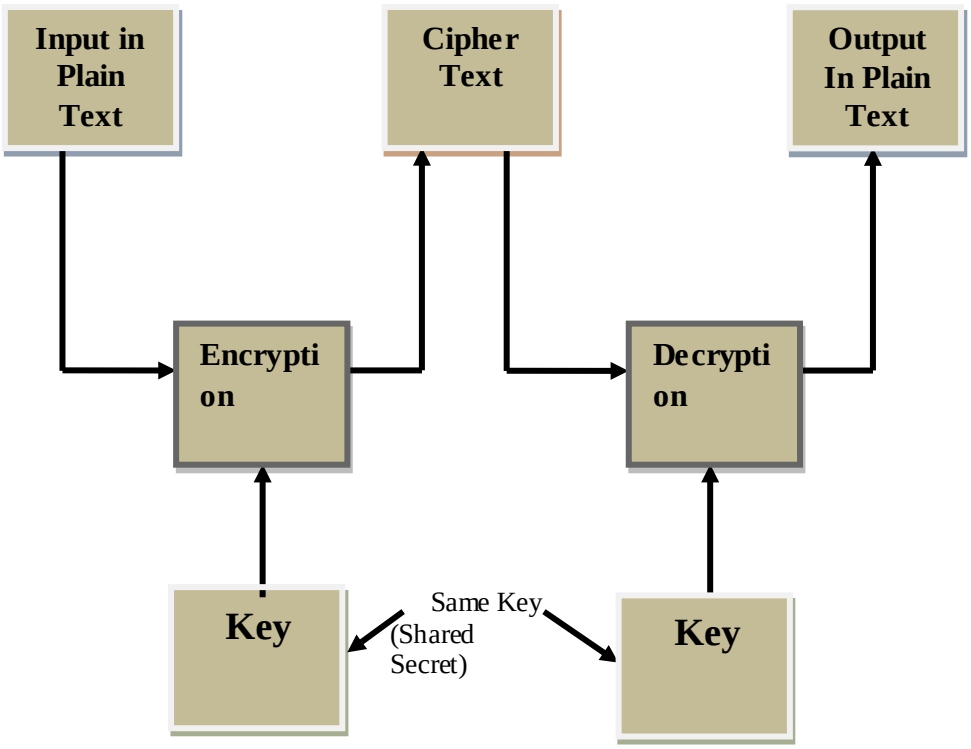


Figure 2.3: Encryption with a Symmetric Key

It's possible that the key used for encryption and decryption are the same, or there may be a straightforward transformation between the two keys. However, the main drawback of this method is that, unlike public key encryption, symmetric key encryption requires both parties to have access to the secret key. The key in this process could be a word or just a random string of letters applied to a message or text. This might be simple to do in order to change content to key in a few specific ways, like moving each letter by number to a different place in the alphabet. AES, DES, HSLE (High-Speed Lightweight Encryption), and SAFAR (Secured and Fast Encryption Routine) are popular symmetric encryption methods.

Asymmetric Key Encryption: In this type of encryption, anyone may encrypt a message, but only the receiver may receive it and have access to decrypt it. A type of asymmetric cryptography is known as public key encryption. In this type of algorithm, we require two types of keys: one is a private key and the other is a public key; in any case, a piece of this key is numerically connected. A public key is requiredat the sender's side, or we may say that to encrypt, we require a public key, and to decrypt cypher text, we require a private key.

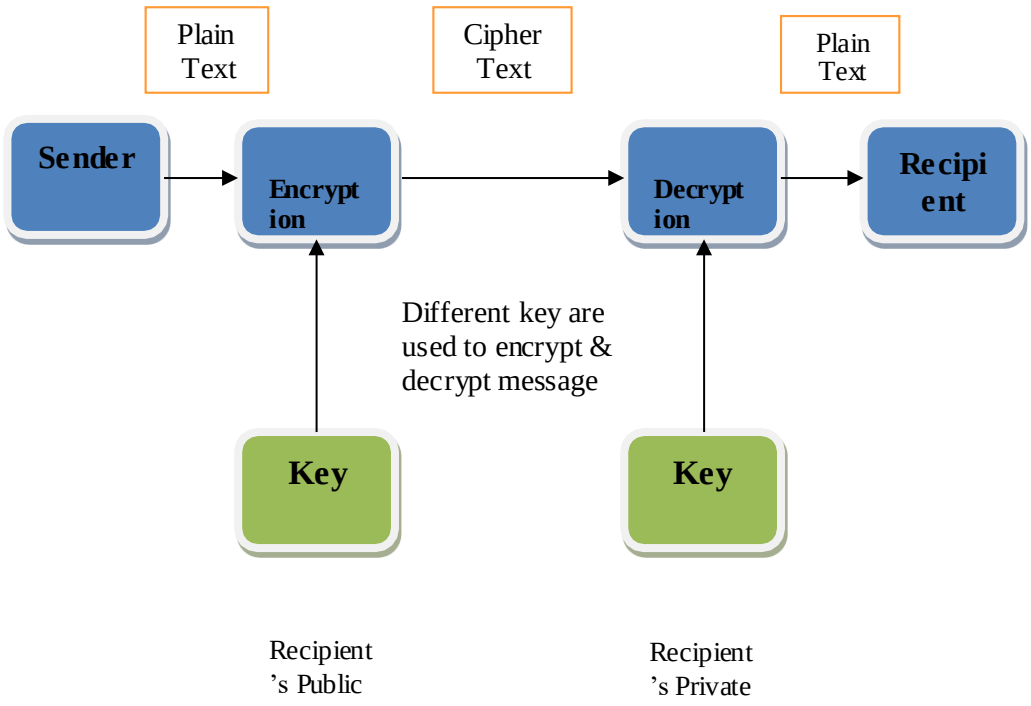


Figure 2.4: Asymmetric Key Encryption

Encryption in Data data-blocks may be categorized as

- Data Message-oriented
- Transaction-oriented
- Session-oriented

LITERATURE REVIEW

3.1 INTRODUCTION

In this literature review, researchers representing their paper on IoT gadgets, for example Rahim Masoudi et al [6] propose that a bunch of exceptional predefined line orders and working frameworks or firmware ought to be utilized. Andrew Whitmore et al [9] work investigates the current state of research on the Internet of Things by reading the writing, identifying the most recent developments, illustrating obstacles to IoT dissemination, introducing open examination questions and future headings, and compiling a comprehensive reference list for specialists. Basudeb Bera et al. [4] The Internet of Drones (IOD) has been widely used in a variety of applications over the past few years, ranging from military to everyday citizen uses. Regardless, during correspondence either with the control room or ground station server(s) or moving entries overhead, security and insurance are vital issues that ought to be taken care of successfully. The clinical Internet of Things (IoT) has significantly improved as a result of the commercialization of 5G, according to Jinquan Zhang et al. [3]. More clinical gadgets associated with the Internet might additionally increase the correspondence power utilization. In the meantime, the security assurance strategy in distributed computing can't match the fast

advancement of clinical applications. In this manner, examining secure, changed, and energy-productive data transmission between clinical devices and cloud servers is undeniably challenging. According to Ambili K. N. et al. [2], with the assistance of IOT (Internet of Things) devices, the world is becoming more connected.

3.2 LITERATURE REVIEW

Sumit Badotra et al [14] examined the fact that the information gathered andput away through IOT gadgets comes from the cloud and consequently, distributed

computing is going about as a spine for supporting IOT. Yet, it is not difficult to fail to remember that the cloud isn't advanced in certain spaces of the world and there is a requirement for a server farm where information stockpiling can be accomplished. Samaresh Bera et al [13] talked about that, Besides, the appearance of programming characterized by organizing (SDN) presents opportunities that permit the organization's administrators and clients to control and access the organization's gadgets from a distance while utilizing the worldwide perspective on the organization.

The Web of Things (IOT) was developed by J. Sathish Kumar et al. [12] and offers the capabilities to perceive and connect real things into a connected system. Personal data access and individual security are real concerns that arise from the Internet of Things. According to Jie Lin et al. [11], fog/edge handling can provide IOT applications with a faster response and a more critical nature of organization in scattered plan and close end clients. Rahim Masoudi et al. recommend a number of distinctive predefined line orders and working frameworks, or firmware. 10]. incorporate touchy and secret data; security concerns have been raised and a couple of researchers are exploring procedures to deal with the security of such contraptions.

Basudeb Bera et al [4] In previous years, the Internet of Drones (IOD) has been broadly utilized for a wide range of applications, from military to everyday citizen uses. Not with standing, during correspondence either with the control room or ground station server(s) or moving sections overhead, security and insurance are vital issues that ought to be taken care of really. On this path, block-chain innovation can be one of the practical arrangements because of the changelessness and discernibility of different exchanges and decentralized nature. In this paper, they give top-to-bottom difficulties and issues regarding the appropriateness of block-chain in the 5G-based Internet of Things (IOT)- empowered IoD climate By incorporating an encrypted calculation and a secure energy-saving correspondence plan into the standard clinical cloud model, they construct a secure energy-saving correspondence and scrambled stockpiling model. In particular, they suggest a Med- Green correspondence confirmation calculation that is elliptic bend and bilinear pair dependent..

In the calculation, the two correspondence groups can complete the essential foundation and character validation in one correspondence, balancing the client's and vital focus's asset overhead and defending against the man-in-the-center attack. They focus on the capacity model for EHR and the security of correspondence in this paper. Based on the Med-Green correspondence confirmation plan and Med- Security calculation, a solid energy-saving correspondence and scrambled stockpiling transmission between IoT devices is a crucial factor in shrewd city administrations' high level of confidence. For example, information that is tampered with would reduce savvy city administrations' dependability, while information that is checked or taken would compromise brilliant city administrations' security. A combination of a k-n secret sharing instrument and programming characterized organizing (SDN) strategy to safely move IoT information was proposed as a means of dealing with secure information transportation among the brilliant city IoT devices for high- certainty intelligent city IoT administrations. Specifically, the data is sent by not entirely set in stone by the SDN controller adaptively. The win big or bust feature of the k-n secret sharing system ensures the security of information. To overcome the challenges of organization state in the Internet of Things, two SDN-based transmission techniques are utilized. Comprehensive analyses conducted from a variety of perspectives demonstrate that the proposed method can significantly reduce the attack success rate with reasonable and adequate overhead. In this paper, that's what they raise, under the ordinary single course transmission framework, data security and transmission trustworthiness can't be guaranteed while defying a data listening attack, especially in an IoT association, which can genuinely hurt the high-assurance wise city IoT organizations (e.g., to diminish the faithful quality and assurance of splendid city organizations). They proposed a multi-course transmission system that encodes the message in multiple privileged insights and communicates insider information through multiple channels in order to strengthen the high certaintyshrewd city IoT administrations.

Using a k-n secret sharing plan prevents an attacker from obtaining any information about the sent information except if she/he compromises countless hubs, which is exorbitant and impossible in reality. Thus, information security has surprisingly improved. Likewise, a multi-course estimation system is proposed to determine the most extreme number of accessible courses. Likewise, a parcel dissemination and resending methodology is proposed to secure against issues like unsteadiness in organization and intruders intentionally disposing of organization bundles. The exhibition evaluation demonstrates that their plan improves the

dependability and protection safeguarding of savvy city administrations expanding upon the IoT network in modern life and provides a significant improvement in the security of information transmission in an IoT network with adequate overhead.

Bin Yuan et al[1] This work develops an SDN network that reduced the network's throughput by re-sending a complete data set in the event of network security attacks. This method took longer than the RSA encryption method to encrypt bytes of data. However, this method is quicker for data in words.

11 milliseconds for l00 node network data transmission. The encoding time for 32 thousand words was 4.30 seconds. Disentangling time for 32K words got 4.11 sec created SDN, which joins a k-n secret sharing system at hubs, in which Information wellbeing is ensured by the go big or go home element of the k-n secret sharing component.

TABLE 3.1 LITERATURE SURVEY SUMMARY

Author(s)	**Title**	**Methodology**	**Research Gap/Limitations**
K. N. Ambiliet al.: [In the Journalof Information Security and Applications, Indexed in 2020]	IoT Networks' Secure Software Defined Networking Framework	used the Wheatstone Algorithm to create a trust-based network connection in SDN to encryptthe data in IoT devices.	The SDN design only consists of 14 fixed nodes,and each node's speed is limited to 10 Mbps. The substitution table used inthe Wheatstone cypher is slower for high-speed SDN. After five seconds, the observe end-to-end delay in 14-node SDN is 2ms.
Bin Yuan and others: 2020, Ordered in IEEE Web of Things]	Software- defined networking andk-n secret sharing ensure the safety of data transportation for high-confidence IoT services.	developed SDN, which combines a k-nsecret sharing mechanism at nodes, ensuring data safety through the k-n secret sharing mechanism's all-or-nothing feature..	In the event of network security attacks, this work creates an SDN network that reduces the network's throughput by sending a complete data set again. This method took longer than the RSA encryption method to encrypt bytes of data. However, this method is quicker for data in words. 11 milliseconds for data transmission in l00 node networks. The encoding time for 32 thousand words was 4.30 seconds.

			Deciphering time for 32K words got 4.11 sec,
Jinquan Zhang and others: 2020, Searchablein IEEE Access]	A RC4-based encrypted storage and secure communication model for HER that saves energy.	Med-Secrecy, based on Huffman compression and RC4, is used to store data. Secu re correspondence confirmation calculation.	Not create SDN Verified using only test suites. For 768 kbs of encrypted data storage, the average amountof time requiredto encrypt the data is 7.5 sec
Basudeb Bera and other individuals:[2020, recorded in the IEEE	Blockchain-based secure data delivery and collection system for the 5G-based Internet of Things	The Web of Drones was their strategy for safe information move. They propose a brand-new secure block- chain framework for sharing executive	SDN has not been implemented in the IoD network. not replicated in a dynamic climate based on SDN. It took a single node 32.084 milliseconds to encrypt data.
Transaction]		information with IoD correspondenc e elements.	

Including Abdullah Al Hayajneh: 2020 Computers Journal]	Software-Defined Networking (SDN): Enhancing the Security ofthe Internet of Things (IoT)	SDN was implemented for safe commu-nication. They developed node using raspberry-pi and utilizationsKodi Media Center and OpenFlow Convention. They offer a man-in-the-middle attack mitigation HTTP encoder.	mitigation only for an attackby a man in the middle. Powerless for assaults like Dispersed Refusalof Administration (DDoS) assaults, SQL infusion assaults and so forth. 92% exactness to keep from man-in-the-center assault in 15(100 Mbps) hub SDN.

When Bin Yuan [1] encrypted a 32K data packet with a secreted data length of 16 bytes, their k-n secrete sharing method encrypts faster than the convectional RSA (Rivest– Shamir-Adleman) method. However, when Bin Yuan [1] encrypted a 32K data packet with a secreted data length of 8 bytes, their methods encrypt slower than the convectional RSA method. The encryption time is not proportional to the size of the data in base work. The size of the data and encryption key should be inversely proportional to the encryption time. Encoding and unraveling should take less time in SDN for constant communication. However, the small size of 8-bit data symbols is always required in the network, particularly in WSN, to interface sensors' signals and map data symbols for communication operations.

In Receptacle Yuan's work, the encryption time isn't straight to the size of the information. The size of the data and encryption key should have a linear relationship with the encryption time. The encoding and decoding times in Bin Yuan's work with SDN for real-time communication may be reduced. Although Bin Yuan Secure Communication has only been tested on 100 SDN nodes with a maximum network speed of 3.52 Mbps, it has the potential to be improved. When a network node is compromised, the likelihood of data compromise should be much lower in Bin Yuan'swork.

In Ambili K N Work Secure mix has been tried on restricted quantities ofhubs (max 14) of SDN with a greatest organization speed of 10 Mbps no one but, it very well may be gotten to the next level. With real-time, high-speed data communication, lightweight data security can be added to the existing blockchain- based secure SDN for additional security. The likelihood of information compromise should be diminished when network hub is compromised.

3.3 SUMMARY

According to the literature review, there are two main methods for encrypting data in Wireless Sensor Networks: RC4 and RSA. Both of these methods require S- Boxes and high-end processor-based nodes for secure communication. We want to use an encryption method that can be done on WSN processors with limited computational power, does not necessarily rely on S-box, and does not make use of slow memory elements. Instead of k-n secrete or RC4, the proposed work employs the High Speed Lightweight Encryption (HSLE) encryption technique and a novel formula-based Data-block data-set finder that is dependent on the given KEY rather than the type of data. The proposed High Speed Lightweight Encryption (HSLE) encryption is best suited to the requirements. Because it does not take a long time to create cipher data, proposed HSLE is capable of real-time data encryption.

METHODOLOGY OF PROPOSED WORK

4.1 HARDWARE and SOFTWARE REQUIREMENT

For completion of the proposed work, hardware and software requirements are asfollows:-

Hardware Requirement: Any hardware that supports MATLAB may be used, generally a general-purpose computer system or a laptop; however, we may also use asmall computer system that exclusively has MATLAB software, like Raspberry-pietc., or in near future asmall controller which has MATLAB Mathematical toolboxand data processing toolbox maybe developed because proposed work requires only adata processing toolbox and mathematical toolbox for MATLAB

Software Requirement: Software required as completion for proposed work is MATLAB anyversion, especially the necessary MATLAB mathematical toolbox, and data processing toolbox, OS may be Window or Linux where MATLAB may install, SCILAB and LABVIEW may also be used as proposed work.

4.2 DESIGN TECHNOLOGY

Secure Software Defined Networking (SDN) data communication and secure data broadcasting, as well as security for private data on cloud servers and any private networks like WSN or WLAN, are the goals of the proposed work, which is a lightweight encryption design. An XOR gate and a key can provide simple security because encryption is all about protecting our data from being interpreted by

outsiders; However, a few simple transform techniques will soon make it clear. Techniques that are difficult to even recognize using transforms or other recursive mathematical solutions must be developed urgently. The goal of the proposed paper is to devise an effective alternative to data encryption for protecting data communication. When data conversion time and encryption time are taken into

account as design parameters, the proposed method is an optimized solution to the same issue. The propose work utilizes the HSLE encryption procedure rather than AES and another recipe based information block informational collection locater which depends on the Vital given and not on the kind of information.

4.3 HIGH SPEED LIGHTWEIGHT ENCRYPTION (HSLE)

Due to its 128-bit key sizes and high security comparable to that of other algorithms, proposed High-Speed Lightweight Encryption (HSLE) is the ideal network intrusion detection system (NIDS) tool to meet the ever-increasing need for speed in today's applications. The proposed work is predominantly founded on planning a productive engineering for low computational capacity regulator base Remote Sensor Organization in Programming Characterize organizing. Block cipher with secret key HSLE is symmetric. The keys to both encryption and decoding should be hidden from unapproved people. Since two keys are symmetric, one might separate the decoding key from the encryption one or the other way around.

The size of the key is fixed at 128 pieces and size of the information block which might be dealt with in one encryption or unscrambling method is fixed to 64 pieces. The HSLE cipher uses 16-bit unsigned integers for all data operations. Padding is required when processing data that is not an integer multiple of a 64-bit block. The security of the HSLE calculation depends on blending three various types of logarithmic tasks: EX-OR, modular multiplication, and addition. A basic function that is iterated eight times is the foundation of HSLE. The first iteration uses a 64-bit plain text block from the input, and subsequent iterations use the 64-bit block from the first iteration. A final transform step generates a 64-bit cipher block following the final iteration. The algorithm structure has been selected in such a way that, with the exception of the utilization of various key sub-blocks, the encryption and decryption processes are identical. Data is encrypted using confusion and diffusion by HSLE. EX-OR, modulo 216 addition, and modulo (216 + 1) multiplication are the three mixed algebraic groups that can all be easily implemented in software and hardware. All of these operations use sub-blocks with 16 bits. The HSLE cipher encryption

process is depicted in Figure 4.1, where M is a modulo multiplier and 'A' is a modulo adder; The Key's K1-K6 parts are 16-bit. In each round to ten rounds of the calculation, the accompanying arrangements of occasions [1] are performed: STEP 1.Modulo Multiply D1 and K1

STEP 2. Modulo Add D2 and K2 STEP 3.

Modulo Add D3 and K3 STEP 4. Modulo

Multiply D4 and K4

STEP 5. The results of XOR are steps 1 and 3. STEP 6. The

results of XOR are steps 2 and 4. STEP 7. Modulo Multiply

Results to Step 5 with K5

STEP 8. Modulo Include the results from step 6 and step 7STEP 9.

Modulo Multiply the results to step 8 with K6.

STEP 10. Modulo Add results to step 7 and step 9STEP 11.

XOR results in step 1 and step 9

STEP 12. XOR results in step 3 and step 9 STEP 13. The

results of XOR in steps 2 and 10

STEP 14. The outcomes of XOR in step 4 and 10

Key Generation:-

The original key is K8, K7, K6, K5, K4, K3, and K1.

Rotate left by 25 bit = K16 K15 K14 K13 K12 K11 K10 K9 Rotate left by 25 bit =K24 K23 K22 K21 K20 K19 K18 K17Rotate left by 25 bit = K32 K31 K30 K29 K28

K27 K26 K25Rotate left by 25 bit = K40 K39 K38 K37 K36 K35 K34 K33Rotate leftby 25 bit = K48 K47 K46 K45 K44 K43 K42 K41

Rotate left by 25 bit = K56 K55 K54 K53 K52 K51 K50 K49Sub-keys

K1-K6 to round two

Sub-keys K7-K12 to round three Sub-keys K13-K18 to round four Sub-keys K19- K24 to round five Sub-keys K25-K30 to round six Sub-keys K31-K36 to round seven Sub-keys K37-K42 to round eight Sub-keys K43-K48 to round nine Sub-keys K49- K52 to round ten

Six sub-keys were required for each of the ten complete rounds, and the final transformation's "half round" required four sub-keys; thus, 52 subkeys were required for the entire procedure. There are eight 16-bit sub-keys that make up a 128-bit key. The 128-bit string is then split into eight 16-bit blocks, each of which contains one of the next eight sub-keys. This shifting and splitting process is repeated until 52 sub- keys are produced. Sub-key repetition is prevented by converting to 25 bits. Six sub- keys are utilized in every one of the 10 rounds. In the ninth "half round" final transformation, the final four sub-keys are used. Six 16-digit key sub-blocks from 128-cycle key. Since the subsequent output transformation requires four additional 16-bit key-sub-blocks, the total number is 52 (= 8 x 6 + 4).

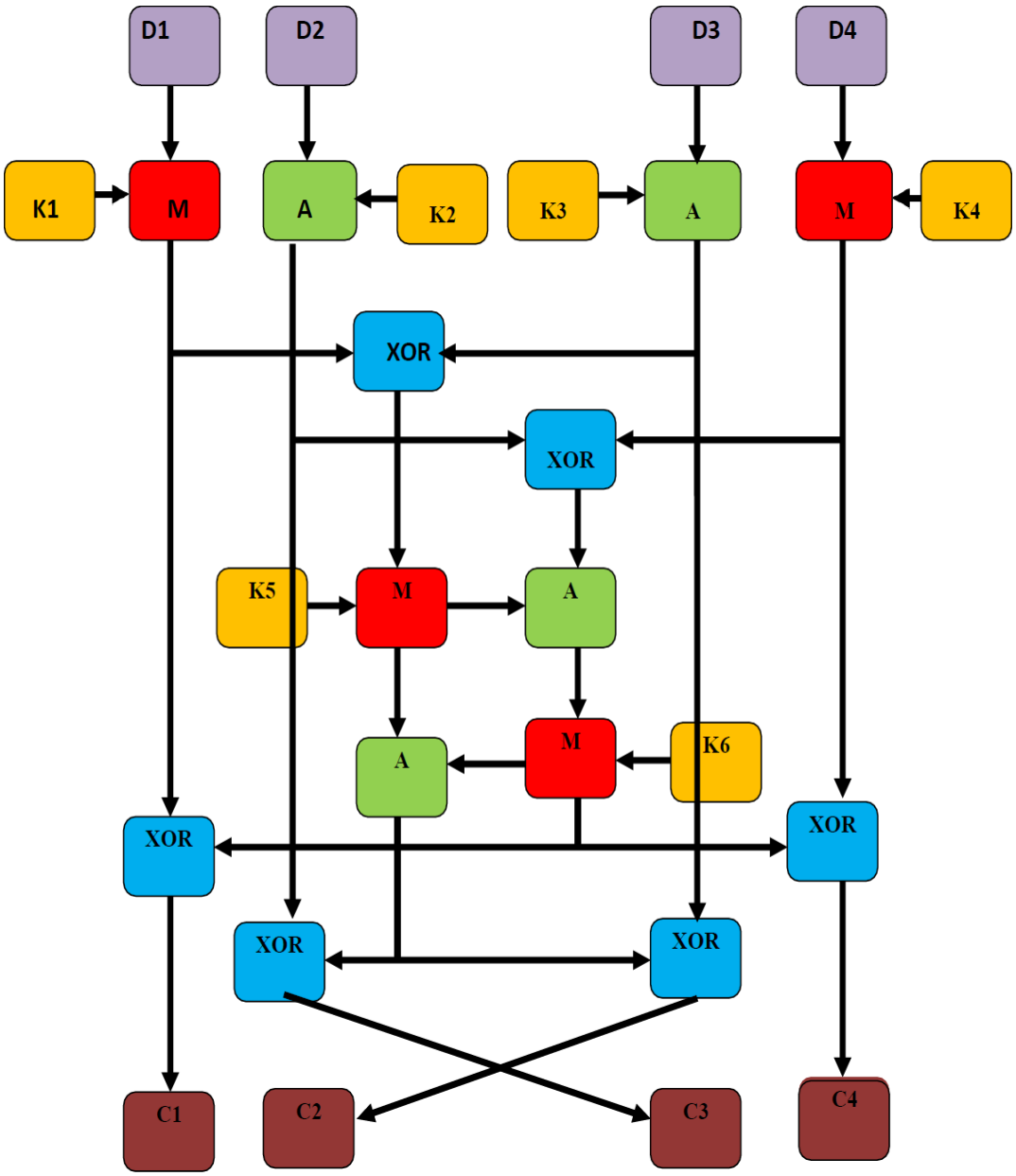


Figure 4.1 HSLE Cipher Generator Module (Proposed work)

First, a 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as firsteight key sub-blocks. 128-bit key is then cyclically shifted to the left by 25 positions after which resulting 128-bit block is again partitioned into eight 16-bit

sub-blocks to be directly used as next eight key sub-blocks. The cyclic shift procedure described above is repeated until all 52 16-bit key sub-blocks have been generated.

Modulo 2^n Adders: Modulo 2^N adders [6] are important to several applications, including residue number systems, digital signal processors, and cryptography algorithms. The modular characteristic to the Residue Number System (RNS) offers potential for high-speed and parallel arithmetic. In RNS logic, each operand is represented by its residues with respect to a set of numbers comprising the base. Addition, subtraction and multiplication are performed in parallel on residues in distinct design units (often called channels), avoiding carry propagation among residues. So, arithmetic operations, e.g., addition, subtraction, and multiplication, may be carried out much more efficiently in RNS than in conventional two's complement systems. That makes RNS a good candidate for implementing a lot of application fields. Typical applications of RNS may be found in Digital Signal Processing (DSP) for filtering, convolutions, correlations, FFT computation, fault-tolerant computersystems, communication, and cryptography. In HSLE 2^16 modulo adder, in use equation below show the operation: -

z= (x + y) mod 2^16 .....Eq. (1)

x and y are inputs, and z is output

Modulo (2^N + 1) multiplier: The symbols for binary numbers with bits are **A = an-1an-2 a0** in the following text, wheren-1A= Σ

$2^i a_i i=0$

A division with a remainder or iterative subtracting modulus until A M can be used toreduce to a number A modulo a number M ("A mod M").

For modulo multiplication, P = X. Y mod (2^n + 1)

One way to calculate the reduction modulo (2n+1) is as follows: A mod (2^n+1) isequal to the (A mod 2^n – A div 2^n) mod (2^n + 1)

4.3.1 Proposed Algorithm

A novel method is used in the proposed work to locate specific network nodes where data must be encrypted, such as with a 128-bit key. Encryption is not required on the network node that is participating in the communication.

KEY=10101011101111101110101011001100101101111110001100111100101011111

Then develop a KEY matrix

$$X0 = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

The Ck coefficient age with the recipe created beneath is givenunderneath, in this model, the quantity of neighbor hubs

considers = 8. It can change based on what the user says.

$$Ck= x(p,1) + x(p+(-1)^k,2) + x(p,3) + x(p+(-1)^k,4) + x(p,5) + x(p+(-1)^k,6) + x(p,7) + x(p+(-1)^k,8 \quad ....(2)$$

p = 1 as k=0 and p=2 as k=1

p = 3 as k=2 and p=4 as k=3

p = 5 as k=4 and p=6 as k=5

p = 7 as k=6 and p=8 as k=7

The coefficients that emerged when we put k at 0, 1, and 7 are shown below.

C0 is composed of x(1,1), x(2,2), x(2,3), x(2,4), x(1,5), x(2,6), x(1,7), and x(2,8).

C1 is composed of x(2,1), x(1,2), x(2,3), x(1,4), x(2,5), x(1,6), x(2,7) and x(1,8)

C2 is composed of x(3,1), x(4,2), x(3,3), x(4,4), x(3,5), x(4,6), x(3,7) and x(4,8)

C3 is composed of x(4,1), x(3,2), x(4,3), x(3,4), x(4,5), x(3,6), x(4,7) and x(3,8)

C4 is composed of x(5,1), x(6,2), x(5,3), x(6,4), x(5,5), x(6,6), x(5,7) and x(6,8)

C5 is composed of x(6,1), x(5,2), x(6,3), x(5,4), x(6,5), x(5,6), x(6,7) and x(5,8)

C6 is composed of x(7,1), x(8,2), x(7,3), x(8,4), x(7,5), x(8,6), x(7,7) and x(8,8)

C7 is composed of x(8,1), x(7,2), x(8,3), x(7,4), x(8,5), x(7,6) , x(8,7) and x(7,8)Neighbor node of network =Min energy(C0, C7, C6, C5, C4 , C3, C2 , C1

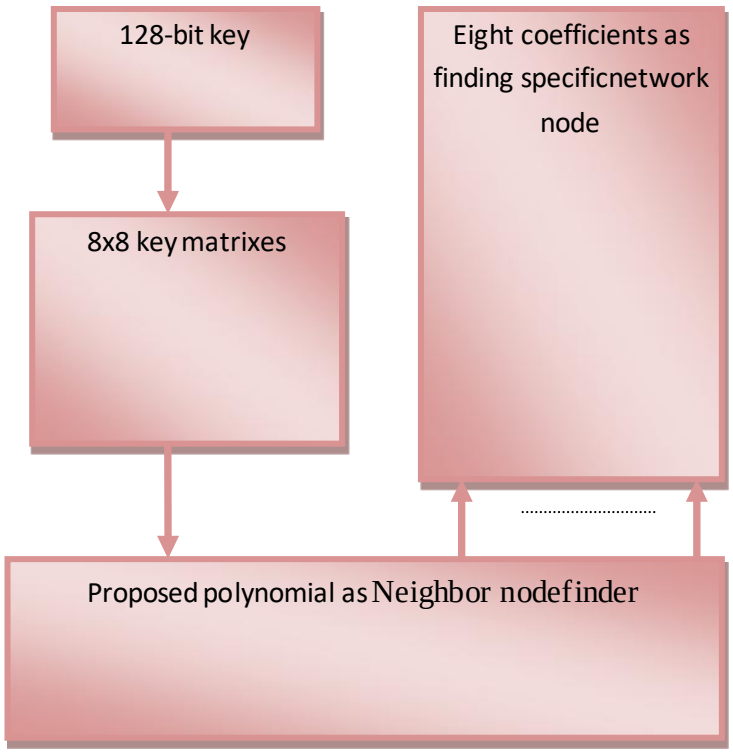


Figure 4.2 Neighbor node Finder (Proposed Work)

4.3.2 Procedures for encrypting data

The overall explanation of the proposed work flow, which can be found in Figure 4.3, can be summarized as follows:

Step 1: Peruse any information from a PC or some other hotspot for WSN climate made with the assistance of MATLAB foster the information as a MATLAB record, and open that document in MATLAB for additional entrance.

Step 2: For a MATLAB-created Wireless Sensor Network, set parameters such as network nodes, neighbor nodes, network range, attenuation factor, and minimum and maximum energy nodes. Here the organization hubs characterize the size of the organization, neighbor hubs are the potential courses that a sending hub can take to

additionally convey the information, weakening component characterizes the hub power blunder resistance level and min and max energy of hubs are utilized to gauge the hub inhabitance in the organization, a high energy consuming hub is viewed as a functioning hub and a low energy consuming hub is yielded free hub for correspondence.

Step 3: Pass any random 128-bit key into the first transmitting nodes and neighbor node finder. There, that key will be further converted into eight polynomials, and then eight different coefficients and their values will be taken into consideration in determining the number of nodes and the minimum energy required for the next transmission.

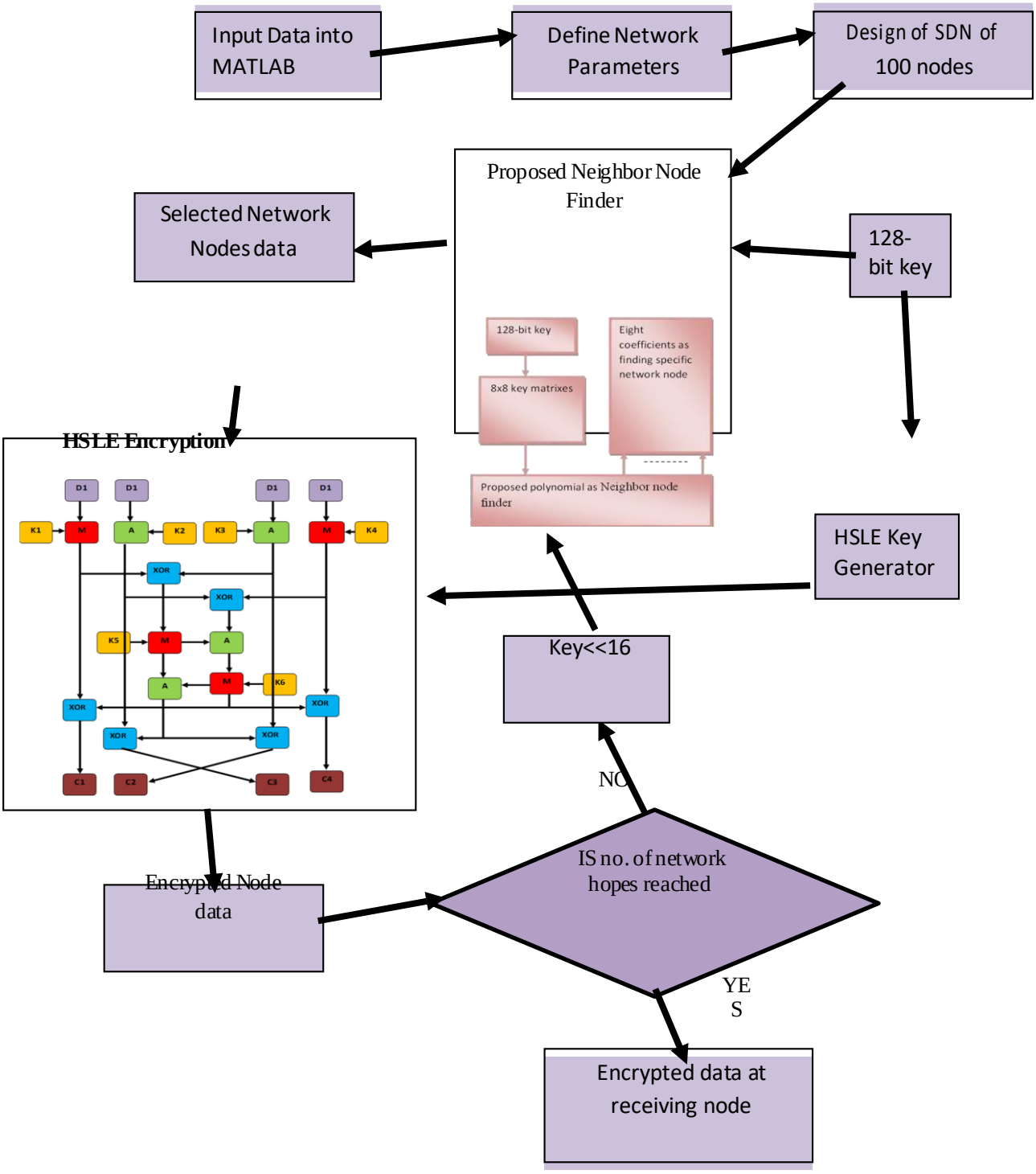


Fig 4.3: Proposed Encryption Procedure (Proposed work)

Step 4: Encode the information utilizing proposed HSLE encryption at the chose hub.

Step 5: Check whether the quantities of expectations for network correspondence have been reached or not, in the event that organization trusts have not been arrived at of course select the following hub with Key left shift by 16 pieces utilizing neighbor hub locater and once more, scramble the following the information on next chose hub.

Step 6: The final ciphers are applied to the data that is received on the destination node once the number of network hopes has been reached.

Step 7: Utilizing the eight coefficients that were discussed in step 3, combine cipher data sets for selected data blocks and unselected data blocks once more.

Step 8: Crypt data is created by combining all modified data blocks in red, green, and blue.

Figure 3.4 below shows that after developing cipher data, it is highly necessary to match the original data and develop cipher data on the basis for standard parameters, here SNR, MSE, and BER are standard parameters taken.

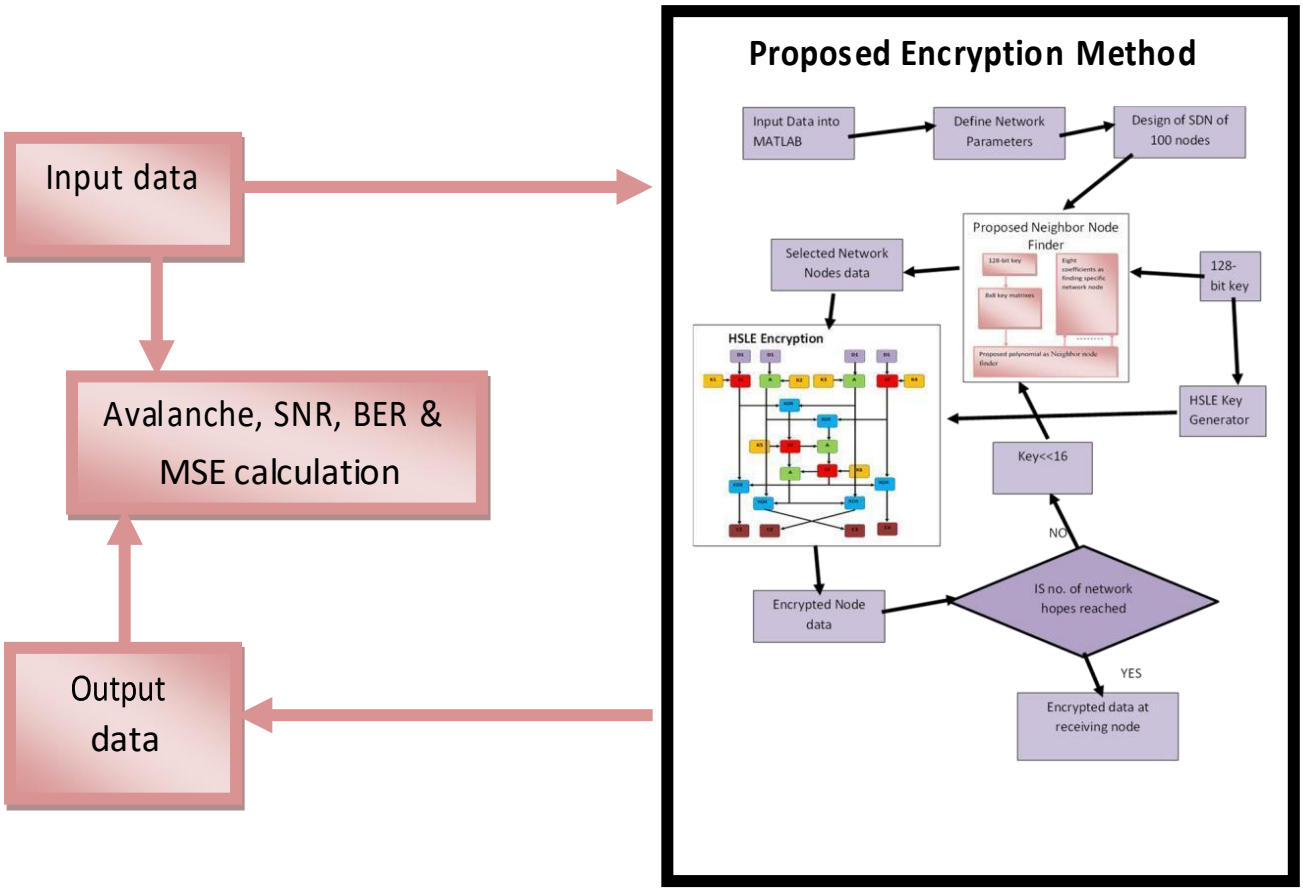


Figure 4.4: SNR between Cipher and Original Data (proposed work)

4.3.3 Original data extraction at Received node

An overall explanation of the proposed work's work flow can be found in Figure 4.5. The following can be used to decipher the flow:

Step 1: The received node's cipher data can be browsed into the MATLAB environment, developed into a MATLAB file, and then opened in MATLAB for further use.

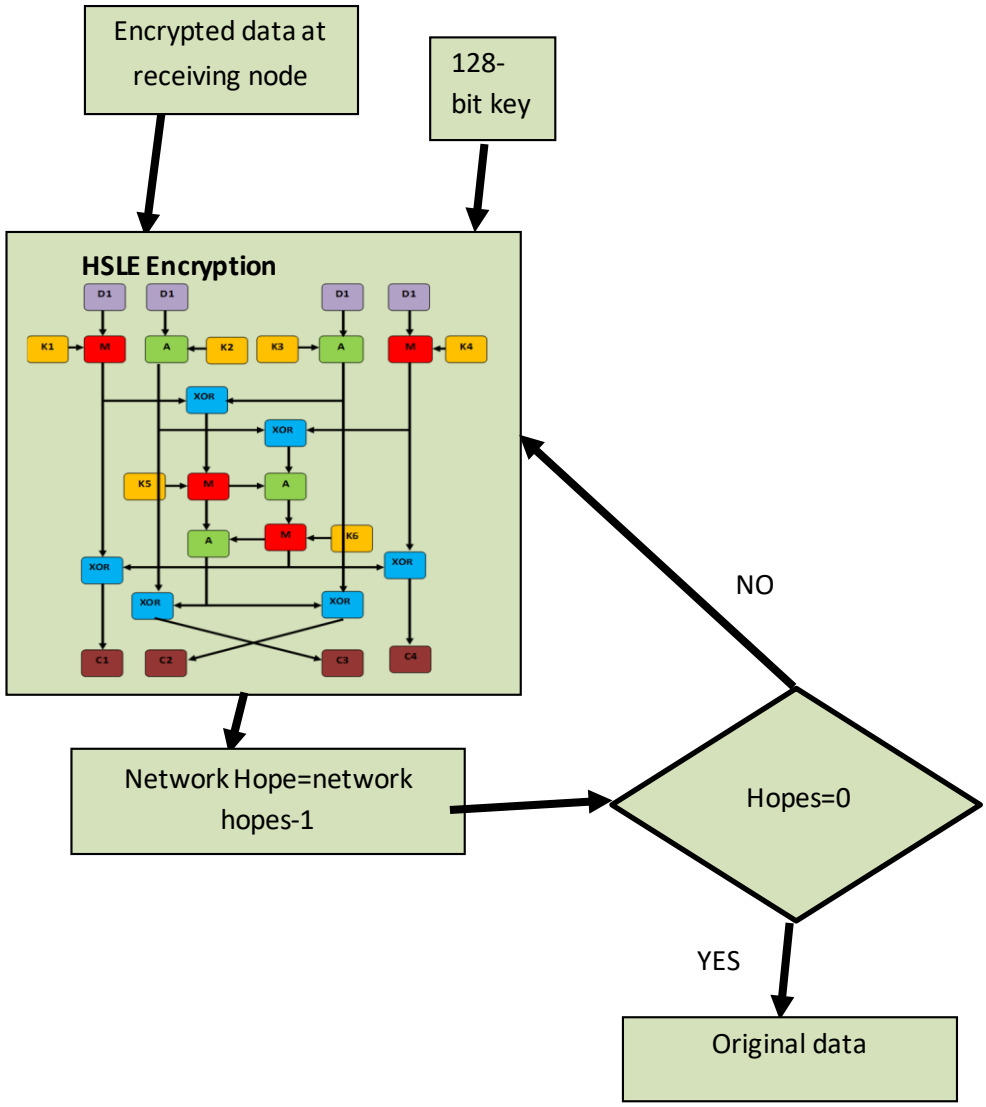


Fig 4.5: Proposed Decryption Procedure (proposed work)

Step 2: Use the same original 128-bit key when applying the HDLE to the received cipher data.

Step 3: Determine whether the network hopes are zero by reducing their count by one. Step 4: If there are more than one network hope, use the HSLE output cipher as data, rotate the key by 16 bits, and repeat the HSLE round.

Step 5: In the event that the quantity of organization trusts is zero, the last round HSLE yield is the gotten unique information.

SIMULATION RESULTS AND DISCUSSION

5.1 INTRODUTION

To execute proposed work programming utilized is MATLAB everything program is written in MATLAB and furthermore tried on MATLAB. Therefore, understanding software is a necessary component of the proposed work. The graphic user interface that was developed for entering network parameters like the number of network nodes, neighbor nodes, range, network attenuation factor, and node minimum and maximum energy threshold is depicted in Figure 5.1 below. Client additionally inputs the 128-bit key and 64-digit information utilizing this GUI. Figure 5.1 shows the outputs as a single network design based on input parameters, encoding and decoding times, and network throughput on nodes. Additionally, the GUI shows the final received cipher on the final received node.

5.2 SIMULATION RESULTS

The graphical user interface was designed as the foreground code for the proposed work. Here the used can provide inputs like data, network nodes, range of network, etc., and keys and outputs are the results parameters like encoding and decoding time.

The graphical user interface that showcases the proposed work for lightweight, high-speed encryption is depicted in Figure 5.1 below. The graphic user interface for entering network parameters, such as the number of network nodes, neighbor nodes, range, attenuation factor, and node minimum and maximum energy threshold, is depicted in this figure. Using this graphical user interface, the user can also enter 64- bit data and a 128-bit key.

Here the organization hubs characterize the size of organization, Neighbor hubs are the conceivable course that a sending hub can take to additionally impart the

information, lessening factor characterizes the hub power mistake resistance level and min and max energy of hub is utilized to gauge the hub inhabitance in the organization, a high energy consuming hub considered dynamic hub and low energy consuming hub surrendered free hub for correspondence.

Pass it to the initial transmitting nodes and neighbor node finder using any random 128-bit key; There, that key will be further broken down into eight polynomials. From those eight polynomials, eight different coefficients and coefficient values based on node number and minimum energy will be chosen for the next transmission.

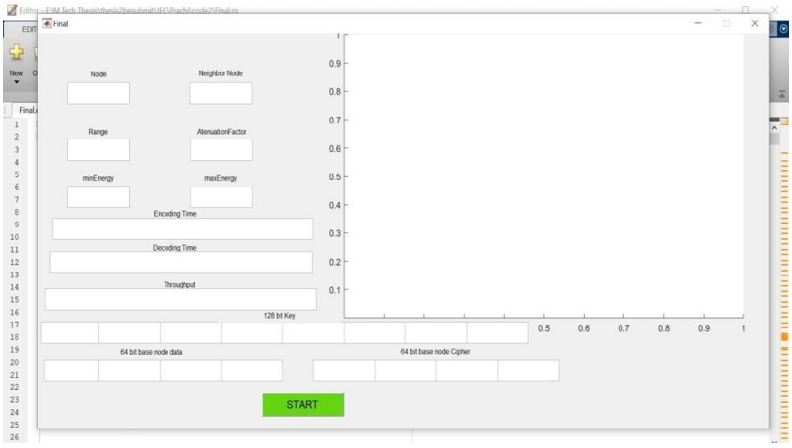


Figure 5.1: GUI develop for user Interface (Proposed work)

The developed graphical user interface for entering network parameters, such as the number of network nodes, neighbor nodes, range, network attenuation factor, and node minimum and maximum energy threshold, is depicted in Figure 5.1 below. This graphical user interface also lets the user enter the 64-bit data and 128-bit key. We can see the outputs as a single network design based on input parameters, encoding and decoding time, and network throughput on nodes in figure 5.1.

The network routing is depicted in Figures 5.2, 5.3, and 5.4 below, with the green circled nodes representing the transmitting and receiving nodes and the green

dots representing the communicating network nodes (network hopes). For safe communication, HSLE (High Speed Lightweight Encryption) is used on each of the network hopes. The dead node is visible on the Red node.

5.2.1 TIME DELAY

It specifies the amount of time it takes for an entire message to reach its destination, beginning with the first bit sent from the source. It consists of the time it takes to send a signal and the time it takes to acknowledge that signal has been received. The propagation times for the paths that connect the two communication endpoints are included in this time delay.So in the proposed work the decoding time (sec) 32kb data is 1.741 which is less than others.

5.2.2 THROUPUT

It determines the number of jobs performed each second. The actual amount of data that is successfully sent or received over the communication link is referred to as throughput. There are a number of technical factors that can cause throughput to differ from bandwidth, such as latency, packet loss, jitter, and more. Throughput is measured in kbps, Mbps, or Gbps. Network Throughput for the proposed work is 10.3Mbps.

The software used to carry out the proposed work is MATLAB. all projects are written in MATLAB and furthermore tried on MATLAB. As a result, the proposed work necessitates an understanding of software. The developed graphical user interface for entering network parameters, such as the number of network nodes, neighbor nodes, range, network attenuation factor, and node minimum and maximum energy threshold, is depicted in Figure 5.1 below

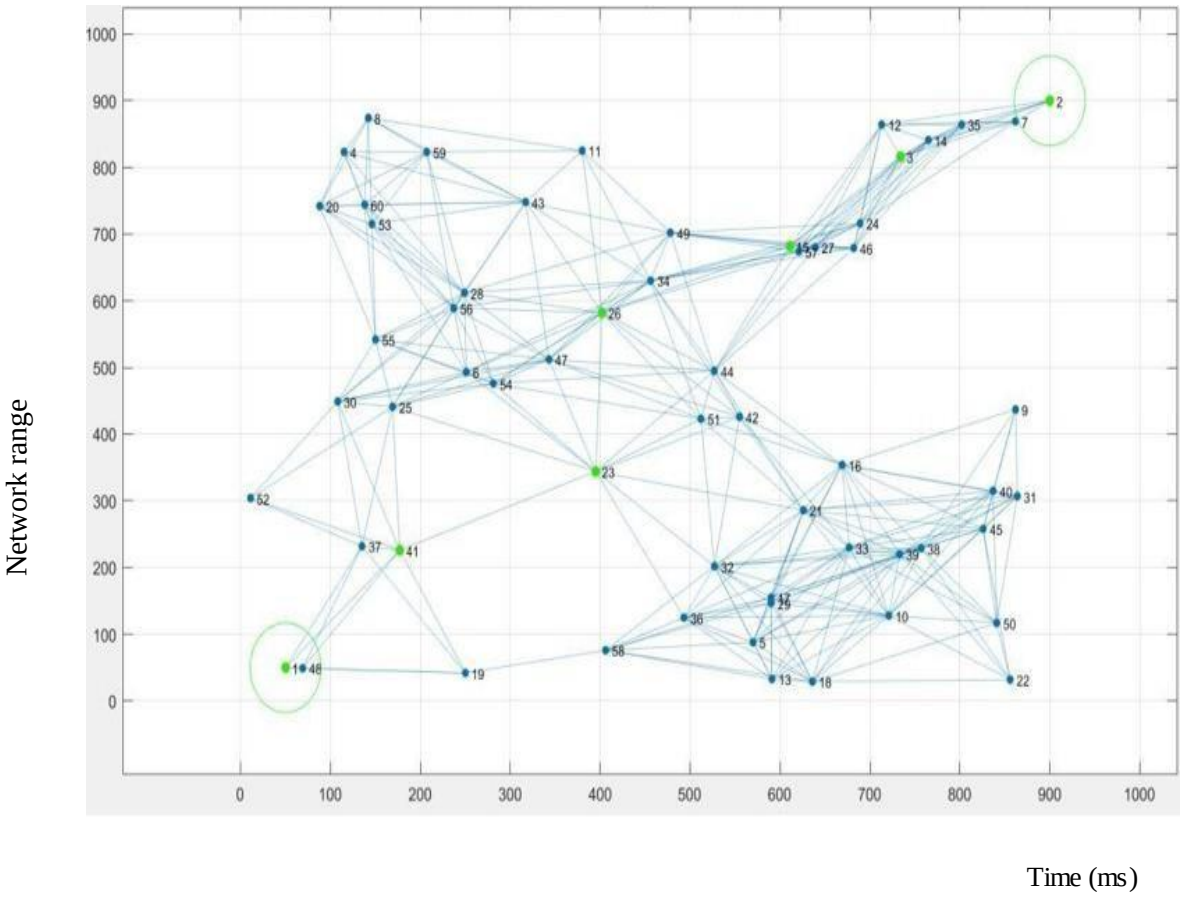
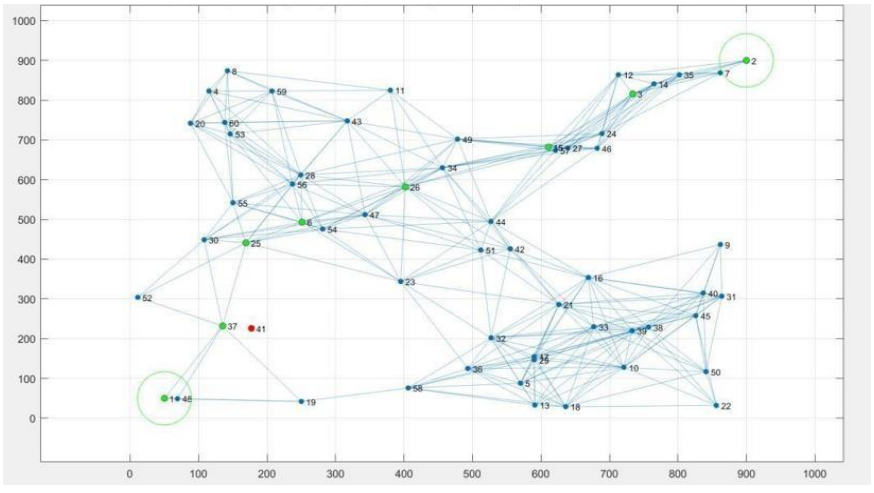


Figure 5.2: Network design with 50 nodes (Proposed work)

We can see the result in figure 5.2, 5.3 and 5.4 we might notice the results as one organization plan according to enter boundaries and encoding and disentangling time on hubs with network throughput additionally we can see the last gotten figure onlast gotten hub in GUI.



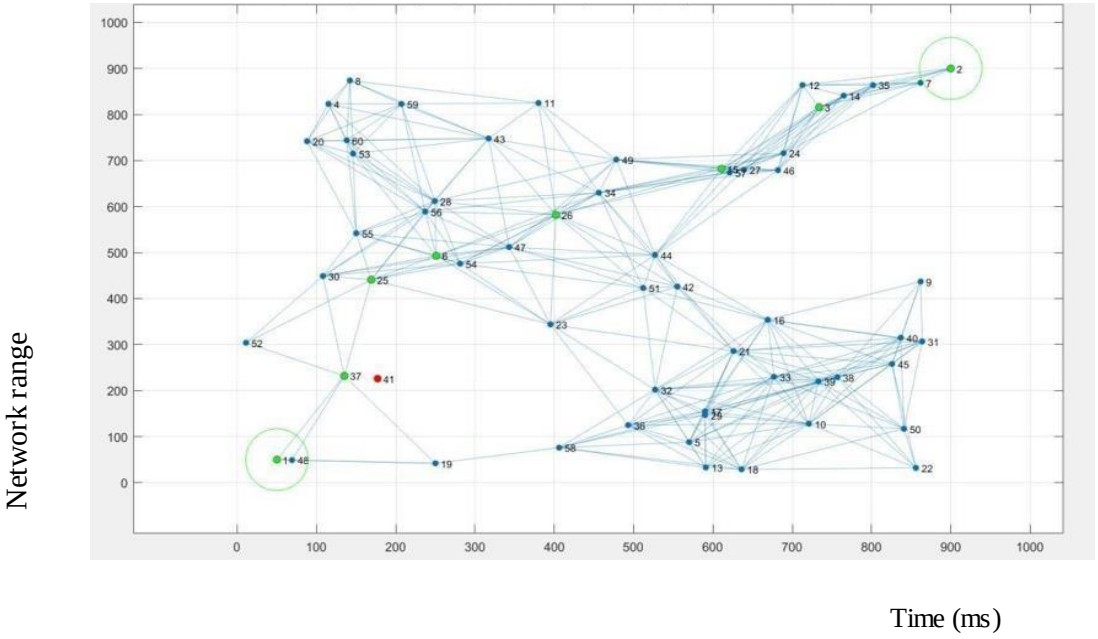


Figure 5.3:Network design with 50 nodes with source and designation nodesdefined(Proposed work

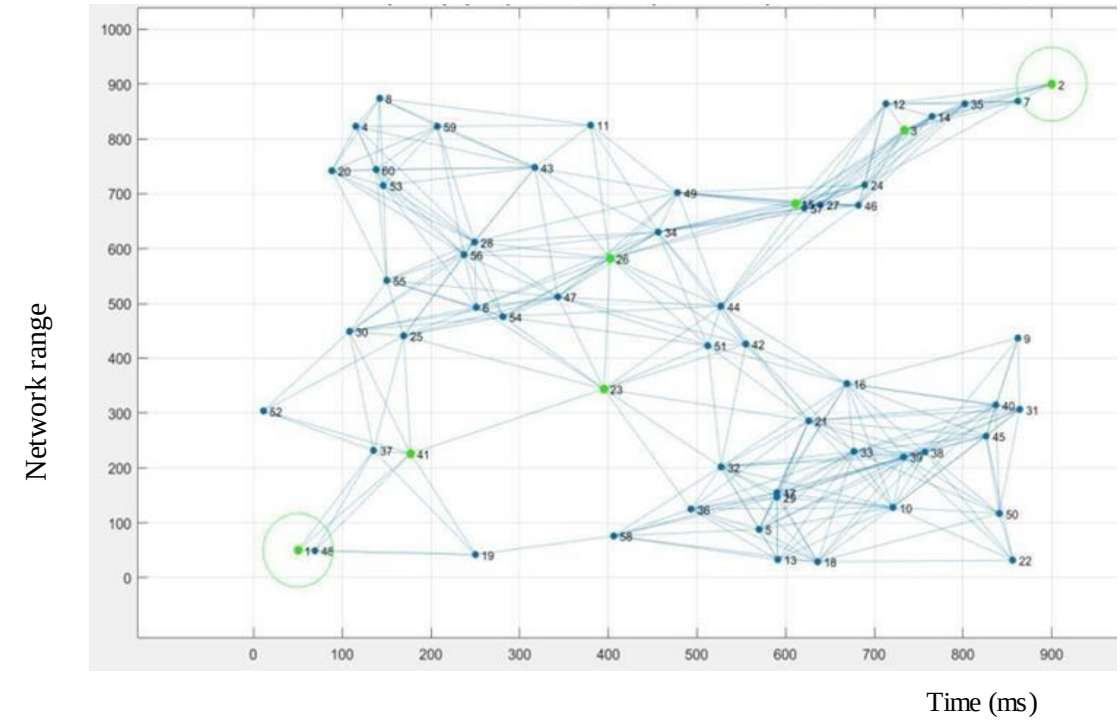


Figure 5.4 Network with corrected routing and encrypted with HSLE(proposed work)

The MATLAB command line output is depicted in Figure 5.5 above. After each round of HSLE, the number of ciphers generated, the packets sent across the network, and the routing nodes chosen using the proposed neighbor node finder are all visible here.

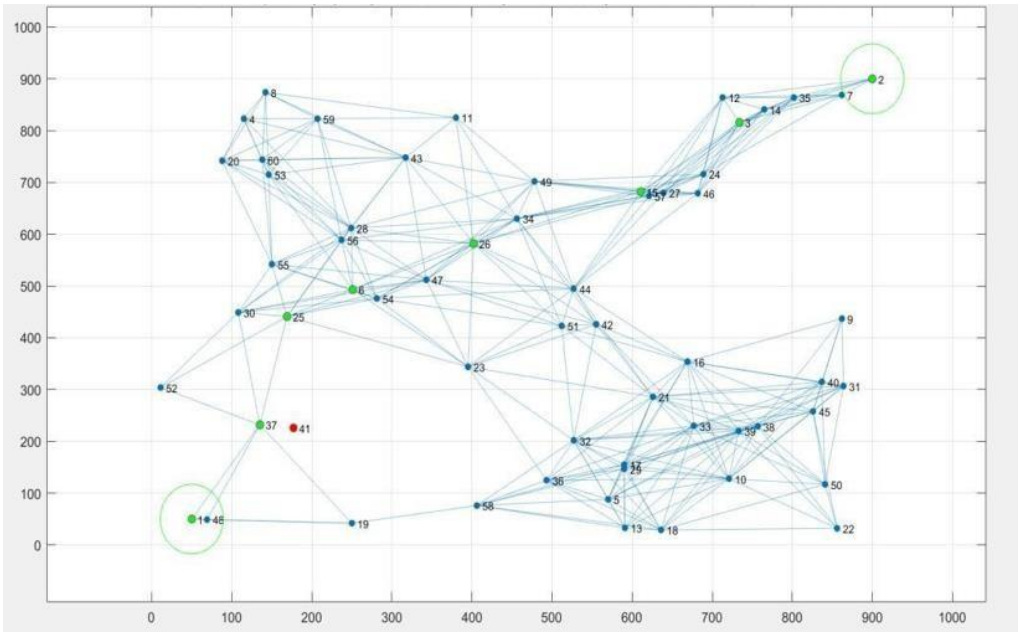


Figure 5.5: Network with 50% sacrifices nodes (Proposed work)

The work has been compared to similar work for secure data encryption. Jinquan zhang et al.[3] reduced time significantly, but they were unable to maintain the level of security because they developed a cipher frame by using simple XOR between selected data blocks. In work by Ambili K. N. et al [2] they were doing AES on pretty much every third information block, which makes their methodology exceptionally impressive against any assault by gatecrashers, yet additionally lessens all out time overwhelmingly and is likewise important for calculations Receptacle Yuan et al. [1] perform encryption on high frequencies just, which rolls out numerous improvements in the first information in the event that any information has a high recurrence part; thus, their method is tremendously subject to the sort of information.

TABLE 5.1: ENCODING TIME OBSERVE FOR PROPOSED HSLE ENCRYPTEDNETWORK NODES

Secrete Data (Kb)	Encoding Time (sec)
128	0.123
256	0.244
384	0.372
512	0.508
640	0.637
768	0.751
896	0.891
1024	1.071
1152	1.308
1280	1.592
1408	1.939
1536	2.342

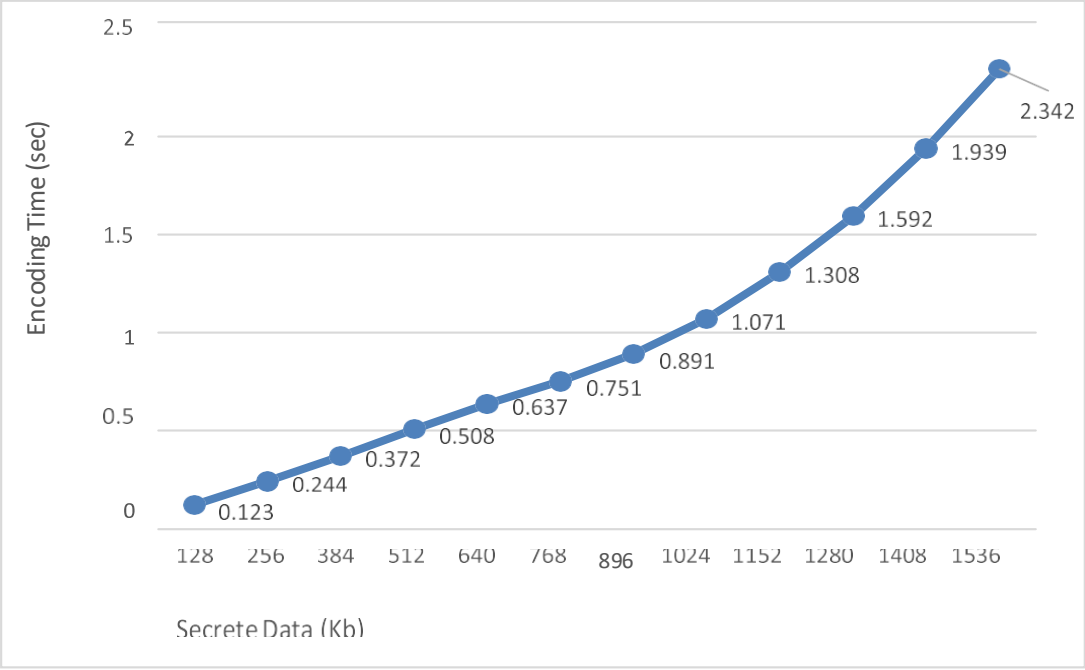


Fig 5.6: Encoding Time observe in HSLE Encryption node (Proposed work)

The proposed network has been simulated with 100 nodes, and for secure communication, HSLE is utilized by all of the proposed network's nodes. The encoding time observed on each node for various sizes of plain text data is depicted inTable 5.1 and Figure 5.7 above

TABLE 5.2: DECODINGTIME OBSERVE FOR PROPOSED HSLE ENCRYPTEDNETWORK NODES

Secrete Data (Kbytes)	Decoding Time (sec)
8	0.617
32	1.741
64	2.982
128	5.573
192	8.032
256	10.03
320	12.79
384	14.08
448	16.92
512	19.15
576	20.63
640	21.82

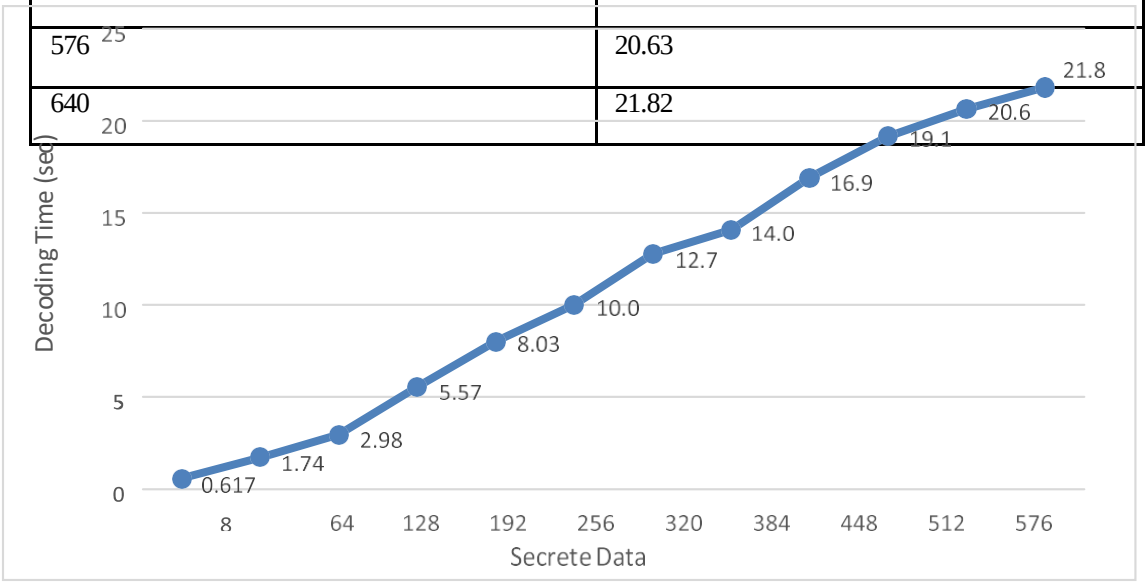


Fig 5.7: Decoding Time observe in HSLE Decryption nodes (Proposed work)

The decoding time that was observed on each node for various sizes of plain text datais depicted in Table 5.2 and Figure 5.8 above.

TABLE-5.3: PROBABILITY OF TRANSMISSION DATA COMPROMISE

Nodes compromised rates	Probability of transmission compromise %
10	0.21
20	1.81
30	5.67
40	10.96
50	16.34
60	25.17
70	35.78
80	49.87
90	68.25

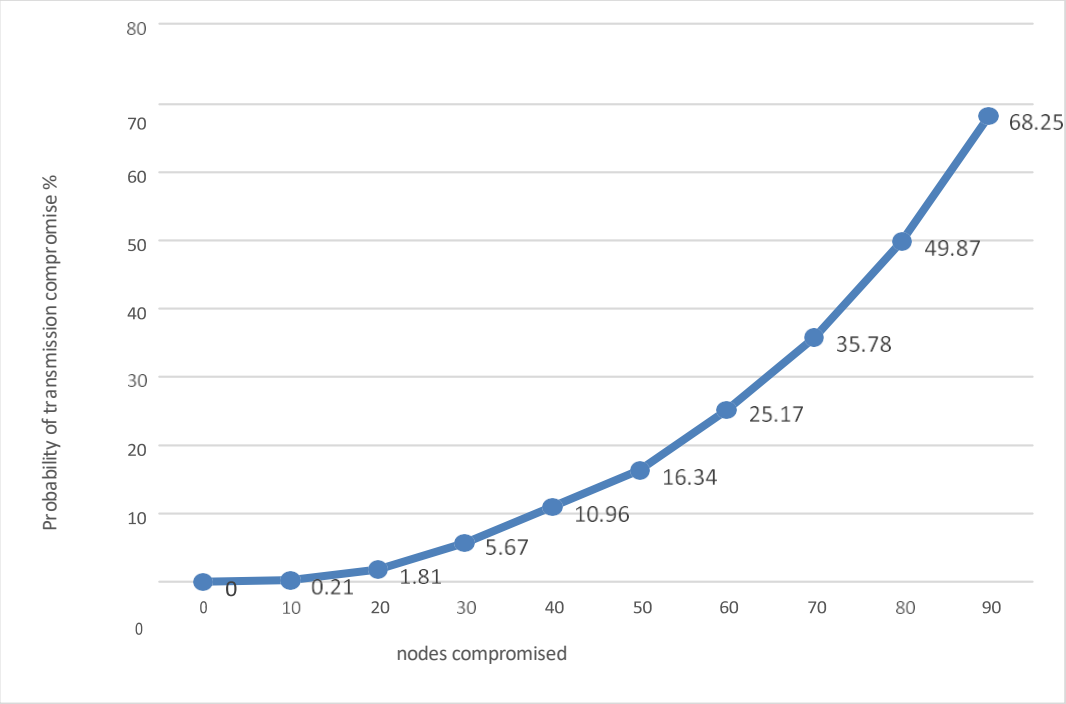


Fig. 5.8: Probability of Transmission Data Compromise when network nodescompromised (Proposed work)

Table-5.3 and figure 5.9 underneath show the Likelihood of sending information compromise when network various quantities of organization hubs compromised in network because of inaccessibility or inhabitance of hubs structure different information correspondence.

5.3 COMPARISON

TABLE-5.4: COMPARISON OF NETWORK NODE ENCODING TIME

Secrete Data (Kb)	Encoding Time (Sec)			
	Proposed work	Bin Yuan [1]	Ambili K N [2]	Jinquan Zhang[3]
128	0.123	1.5	3.2	0.125
256	0.244	4.5	7	0.3
384	0.372	5.5	9	0.6
512	0.508	7.5	11	0.87
640	0.637	9	16	1.2
768	0.751	11	19	1.5
896	0.891	13	-	-
1024	1.071	16	-	-
1152	1.308	17.5	-	-
1280	1.592	20	-	-
1408	1.939	21	-	-
1536	2.342	24	-	-

Comparative encoding times for various data sizes encrypted on each node in a proposed HSLE-based network with 100 nodes are shown in Table-5.5 and Figure-

5.10 below. This work performs better than others because it employs HSLE, which is

faster than other methods. The relative decoding times for various sizes of data decrypted on the final receiving node in the proposed HSLE-based network of 100 nodes simulated in MATLAB 2018 are depicted in Table 5.6 and Figure 5.11. Because it uses HSLE, which is faster than other methods, this work required less time to decode the data.

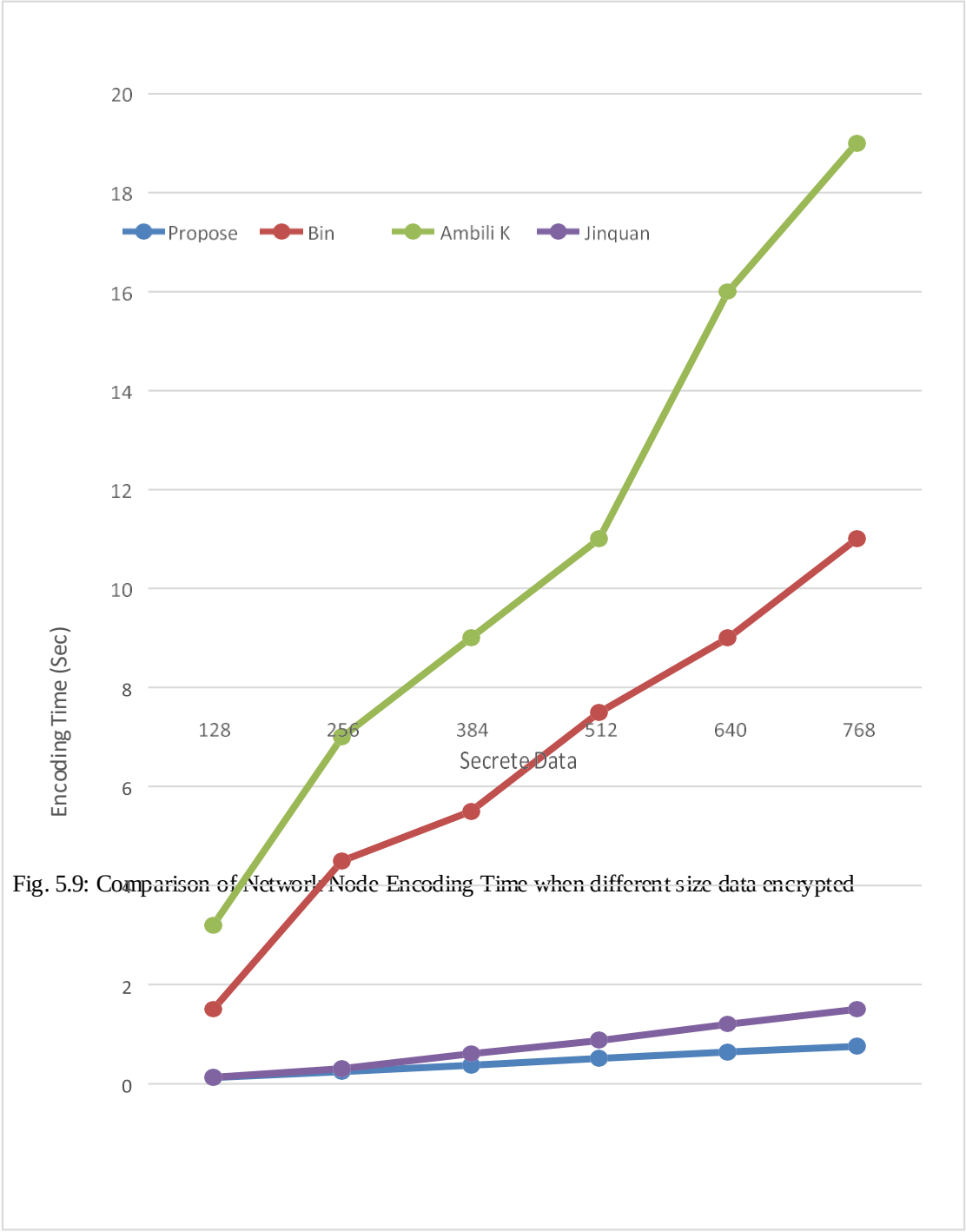


Fig. 5.9: Comparison of Network Node Encoding Time when different size data encrypted

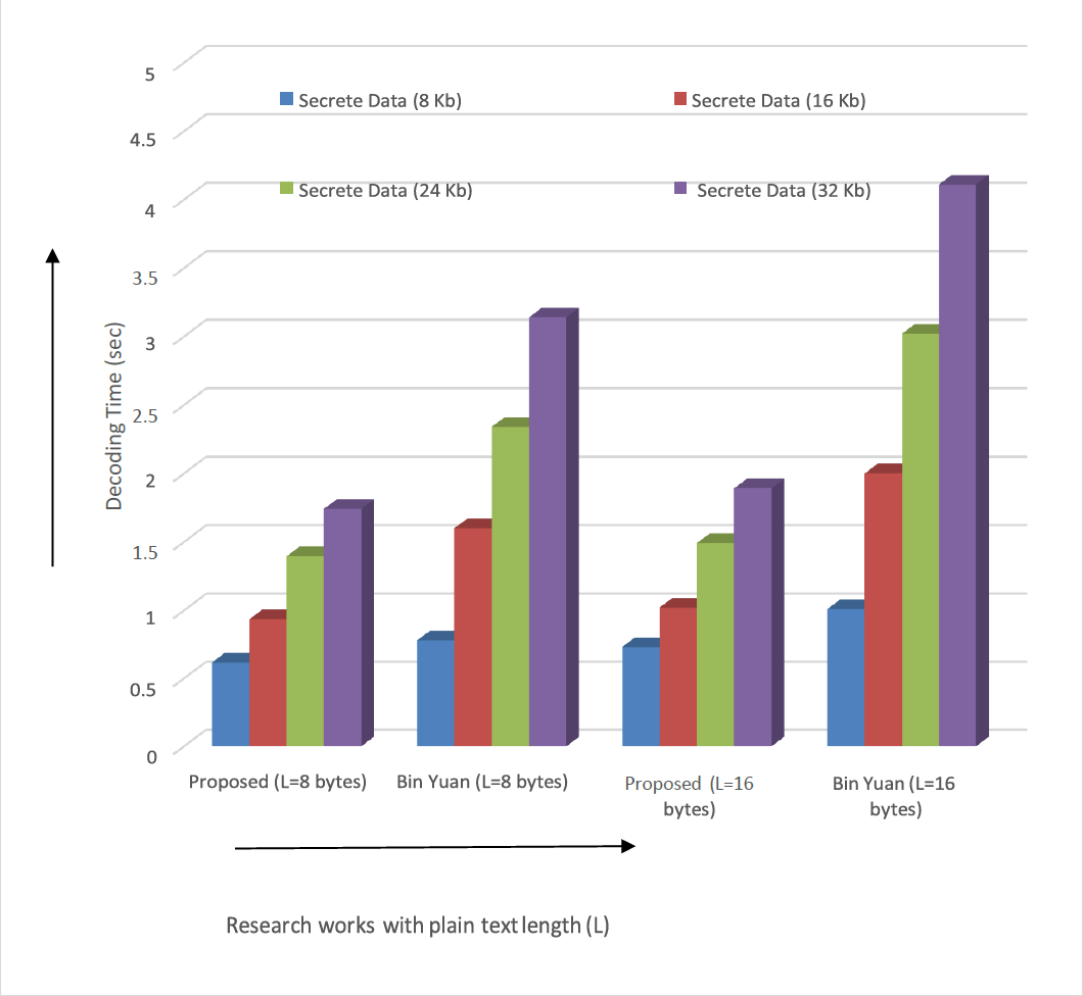


Fig. 5.10: Comparison of Network Node Decoding Time when different sizedata Decrypted (Proposed work)

TABLE-5.5: COMPARISON OF NETWORK NODE DECODING TIME

Secrete Data (Kb)	Decoding Time (sec)			
	Proposed		Bin Yuan [1]	
	L=8 byte	L=16 byte	L=8 byte	L=16 byte
8	0.617	0.732	0.78	1.01
16	0.935	1.021	1.6	2
24	1.395	1.492	2.34	3.02
32	1.741	1.892	3.14	4.11

TABLE-5.6: COMPARISON OF TRANSMITTING DATA COMPROMISSION

Numbers of Nodes Compromised	Probability of transmission compromise %	
	Proposed	Bin Yuan [1]
0	0	0
10	0.21	0.35
20	1.81	3.09
30	5.67	8.41
40	10.96	16.91
50	16.34	27.42
60	25.17	39.87
70	35.78	53.91
80	49.87	68.31
90	68.25	83.41

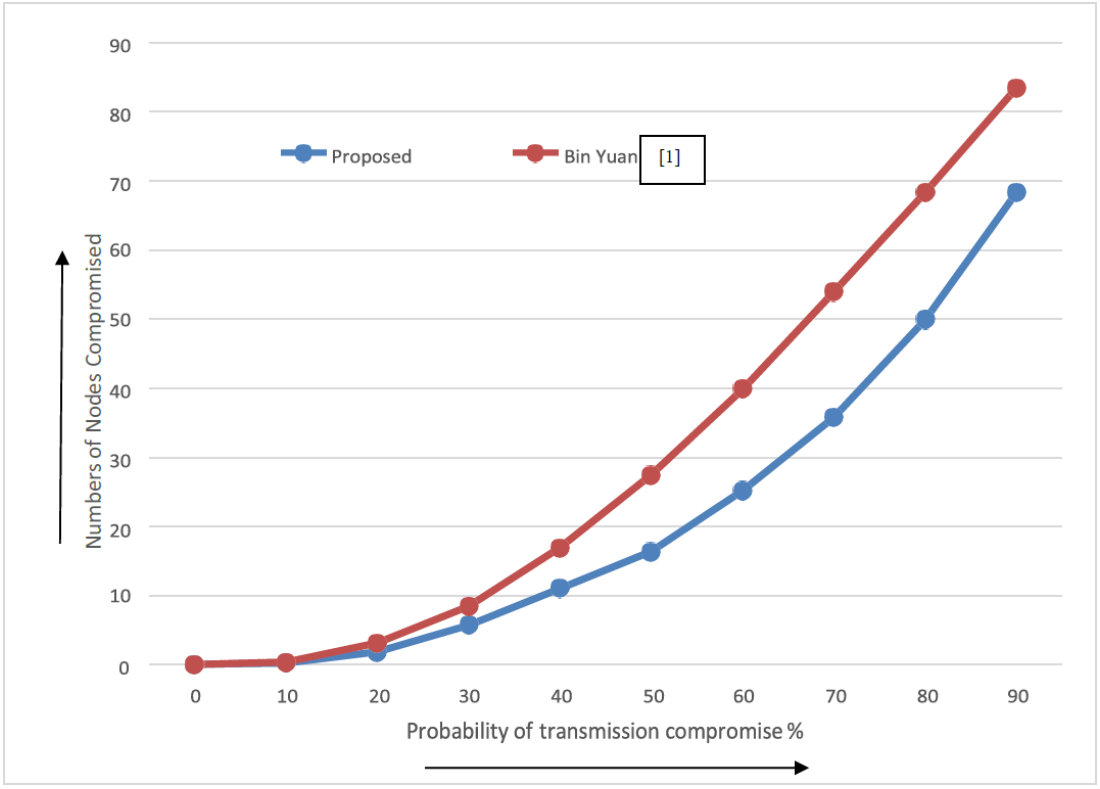


Fig. 5.11: Transmitting data compromission comparison when different numbers of network nodes get compromised (Proposed work).

Comparative results between the proposed HSLE encryption and other encryption methods for a 100-node MATLAB network are presented in Table 5.6 and Figure 5.12. When a large number of network nodes are compromised due to high traffic, the probability of data compromise is shown in Table 6. It could be seen when 10% hubs in an organization are compromised in the likelihood of information compromission noticed for proposed work is just 0.21 which is least among different strategies, likewise when 90% of organization hubs get compromised the likelihood of sending information to get compromission is just 68.25% which is again least in contrast and different works, subsequently it very well might be said the proposed HSLE encryption-based network is more dependable than different organizations.

The work has been contrasted and comparative work for secure information encryption, jinquan zhanget al[3] diminished time overwhelmingly, yet couldn't keep a high security level since they were utilizing simple RSA between chose information blocks to foster code information. In the work of K. N. Ambili et al. 2], they were performing RC4 on nearly every third data block, which not only makes their method extremely resistant to any intruder attack but also significantly shortens the total amount of time required for computations and requires m. Bin Yuan and others [1] perform encryption on high frequencies just, which rolls out numerous improvements in the first information in the event that any information has a high recurrence part; thus, their method is tremendously subject to the sort of information. Table 7, displayed underneath, shows relative outcomes acquired from the proposed work and other workthat pre-owned standard information as their recreation.

$$Throughput\ in\ [1] = \frac{0.8Y10^{-6} * 2^{20}}{2 * 2^{10}} = 6.4\,Mbps$$

TABLE 5.7 COMPARATIVE RESULTS (Proposed work)

Parameter	Proposed	Bin Yuan et al [1]	Ambili KN et al [2]	Jinquan zhang et al[3]
BER	0.54	0.6725	-	-
Probability of transmission compromise % (50 nodes)	16.34	27.42	-	-
Decoding Time (sec) 32kb data	1.741	3.14	5.34	**1.98**
Encoding Time (sec) 128 kb Data	0.123	1.5	3.2	**0.125**
Network Throughput (14 Node Network)	**10.3 Mbps**	**6.4 Mbps**	**10 Mbps**	-

Table-5.7 displayed underneath shows near results acquire as proposed work and other work which involved standard Information as their reenactment. Figure 5.13 shows a comparison of the network throughput. It can be seen that this work has a higher throughput than other works due to the quick HSLE encryption method and faster encoding and decoding times.

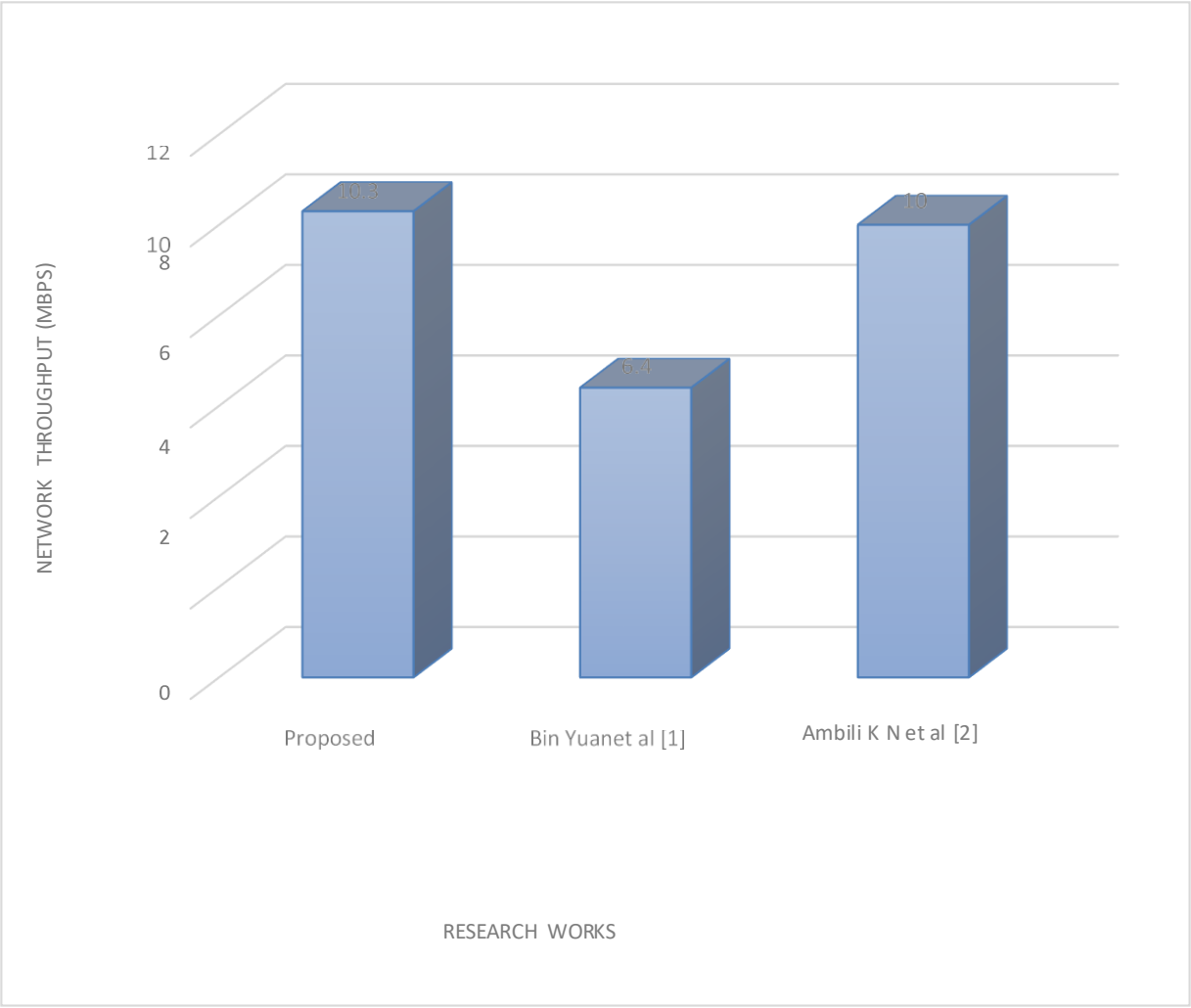


Fig 5.12: Comparison of Network throughput (Proposed work)

CONCLUSION AND FUTURE ASPECT

6.1 CONCLUSION

By modifying existing methods, such as encrypting data with probabilistic encryption, this work proposes a high-speed lightweight encryption (HSLE) base security scheme for wireless sensor networks that reduces overhead in terms of latency. The proposed work is likewise helpful when we convey our classified information or information on WSN, so it will be secure. We only need to save encrypted data on a few WSN nodes. The proposed work is another key-based calculation to figure out information blocks and explicit informational indexes in information and use HSLE encryption rather than AES. Proposed strategies cause huge speed improvement for information encryption with comparable security; Additionally, they are ideal for hand-to-hand communication between mobile phones, palmtops, and other similar devices. Algorithm can be used between sites where effective encryption is essential and processing power and battery power are limited. The proposed work has the shortest encoding time of all the works that are available and the highest BER of all the works that are available. The proposed algorithm's future component is designed as a decryption procedure. The military as well as highly secure data communication could benefit from this thesis's implementation. MATLAB was used to complete this thesis work. MATLAB is used to simulate the proposed work; In the future, work might be done with much more advanced software tools that have a lot of computational power but less memory, making it easier to work quickly. Numerous stages of encryption may be added in the near future; However, due to the fact that adding multiple stages will increase time delay and decrease throughput, it should be done with extreme caution.

6.2 FUTURE WORK

The proposed algorithm's future component is designed as a decryption procedure. This thesis's work could be used for high-security data communication and the military. MATLAB was used to complete this thesis work. MATLAB is used to simulate the proposed work; In the not-too-distant future, work might be carried out using much more advanced software tools with hardware that has a lot of computational power but less memory to speed things up. Numerous stages of encryption may be added in the near future; notwithstanding, it ought to be exceptionally cautious in light of the fact that adding many stages will increment time delay and decrease throughput.

REFERENCES

[1].B. Yuan et al., "Secure Data Transportation with Software-Defined Networking and k-n Secret Sharing for High-Confidence IoT Services," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7967-7981, Sept. 2020, doi: 10.1109/JIOT.2020.2993587.

[2].Ambili K N, Jimmy Jose, "A Secure Software Defined Networking based Framework for IoTNetworks", in Journal of Information Security and Applications, Vol.1, no. 1, Sept. 2020, pp: 532-539.

[3].J. Zhang, H. Liu and L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR," in IEEE Access, vol. 8, pp. 38995-39012, 2020, doi: 10.1109/ACCESS.2020.2975208.

[4].Haojie Shen, Li Zhuo, Yingdi Zhao, an efficient motion reference structure based selective encryption algorithm as data's, Published in IET Information Security, IET Inf. Secure, 2014, Vol. 8, Issue 3, pp. 199–206, Institution for Engineering and Technology 2014, doi: 10.1049/iet-ifs.2012.0349

[5].M. Li, C. Yang and J. Tian, "Video Selective Encryption Based on Hadoop Platform," 2015 IEEE International Conference on Computational Intelligence & Communication Technology, 2015, pp. 208-212, doi: 10.1109/CICT.2015.122.

[6].A Massoudi, F Lefebvre, C De Vleeschouwer, B Macq and JJ Quisquater, "Overview on Selective Encryption for Data and Data: Challenges and Perspectives", EURASIP Journal on Information Security, vol. 2, no.5, May-2018, pp: 223-232.

[7].W. Puech, A. Bors and J.M. Rodrigues, "Protection for Color Data by Selective Encryption", IEEE Transaction on Circuits and Systems for Video Technology, vol. 9, no. 4, pp:551–564, Apr. 2013.

[8].Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More, Proposed Data Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study, International Journal for Computer Applications, Volume 65– No.1, March 2013, pp:0975 – 8887.

[9].D. He, C. Chen, S. Chan, J. Bu and L. T. Yang, "Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks", *IEEE Trans. Ind. Electron.*, vol. 60, no. 11, pp. 5348-5354, Nov. 2013.

[10]. C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu and L. T. Yang, "Trust- based communication for the industrial Internet of Things", *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16-22, Feb. 2018.

[11]. M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues", *Proc. IEEE Int. Conf. Privacy Security Mobile Syst.*, pp. 1-8, 2014

[12]. R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of Things (IoT) security: Current status challenges and prospective measures", *Proc. 10th IEEE Int. Conf. Internet Technol. Secured Trans.*, pp. 336-341, 2015.

[13]. F. A. Rahman, M. Daud and M. Z. Mohamad, "Securing sensor to cloud ecosystem using Internet of Things (IoT) security framework", *Proc. 2016 ACM Int. Conf. Internet Things Cloud Comput.*, pp. 1-5, 2016.

[14]. Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin and K. Ren, "Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy", *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 4, pp. 591-606, Jul./Aug. 2018.

[15]. D. Zhang, L. T. Yang, Z. Chen and P. Li, " PPHOPCM: Privacy-preserving high-order possibilistic c -means algorithm for big data clustering with cloudcomputing ", *IEEE Trans. Big Data*, May 2017.

[16]. Patil Ganesh G and Madhumita A Chatterjee, Selective Encryption Algorithm as Wireless Ad-hoc Networks, International Journal on Advanced Computer Theory and Engineering (IJACTE), ISSN (Print) :2319 – 2526, Volume-1,Issue-1, 2012

[17]. Ajay Kushwaha, Enhancing Selective Encryption Algorithm as Secured WSN, 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation, 2166-8531/2012 IEEE, DOI 10.1109/CIMSim.2012.16

[18]. Pavithra. C Vinod. B. Durdi, Analization and Comparison for Selective Encryption Algorithms with Full Encryption as Wireless Networks, International Journal for Engineering Trends and Technology (IJETT) – Volume 4 problem 5- May 2013, ISSN: 2231-5381 Http://www.ijettjournal.org Page 2083[19].Wireless sensor network

(WSN) – GeekforGeeks (Google) [20].