International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I11P112

Volume 72 Issue 11, 91-98, November 2024
© 2024 Seventh Sense Research Group®

Original Article

Development of a Conceptual Model for Secured Communication in Wireless Ad hoc Networks

S. Vandana[1], Madhavi Tatineni[2]

[1]*Department of Electronics and Instrumentation, VNR Vignana Jyothi Institute of Engineering and Technology, Telangana, India.*
[1,2]*Department of Electrical, Electronics and Communication Engineering, GITAM School of Technology, Telangana, India.*

[1]*Corresponding Author : vandana_s@vnrvjiet.in*

Received: 15 July 2024 Revised: 20 October 2024 Accepted: 29 October 2024 Published: 29 November 2024

***Abstract* - In wireless ad hoc networks, secure data transfer is crucial. Providing a high level of security for security-sensitive operations, such as military and defense applications, is essential. Existing cryptographic techniques and routing protocols, such as AODV, DSR, encryption, and decryption algorithms, cannot offer high-end security. So, a conceptual model was created where 3-levels of data encryption provide high-end security. The receiver's unique ID was used to provide security in the first level; random key generation was used in the second level, and a polynomial equation was produced in the third level to enhance security further. Security is provided at each level so that eavesdroppers cannot decipher it. Only the authorized end user can decrypt, as the key for decryption will be only with the authorized user. The method was used to successfully deliver encrypted data from the transmitter to the receiver, where it was then successfully decoded.*

***Keywords* - Receiver's unique ID, Random key generation, An eavesdropper, Ad hoc Networks, Cryptographic techniques.*

1. Introduction

Wireless networks have replaced wired networks because of technological developments in communication systems. Wireless Ad hoc networks are wireless networks that do not have a fixed infrastructure. A wireless Ad hoc Network is a group of nodes that can build a temporary Ad hoc network without using any existing network infrastructure, with each node acting as a router that stores and sends packets to the destination. They are prone to security concerns due to a lack of established infrastructure. Ad hoc networks are mainly used for military tactical and other security-sensitive operations. However, the use of ad hoc networks for commercial purposes is on the rise due to their unique characteristics. Secure data communication has three core principles: confidentiality, integrity, and availability. These concepts form a model and framework for data security. Confidentiality confirms that data is accessed only by authorized users with the proper credentials. Integrity verifies that data is reliable, accurate, and not subject to unwarranted changes. Availability ensures data is readily and safely accessible and available for ongoing needs. To enable narrowband communication and create a network with end devices, the open-source 802.11 module's firmware must be updated. In COTS-based systems, effective utilization of bandwidth was demonstrated by allocating a narrow bandwidth of 1 MHz to a Node. The data was communicated between the Server and 9 nodes effectively. Even though Narrow Band Communication is secure, the vulnerability of these networks to security threats is the fundamental challenge in their design. As a result, it is necessary to establish a mechanism that can securely handle ad hoc networks. This paper shows the secure mechanism to protect any ad hoc network, giving 3 levels of security.

2. Literature Review

Narrow-band subliminal channels channel capacity is assessed when a transmitter only attempts a controlled number of inputs. Secret message-embedded data is applied to a model where successive transmission of carriers was done. The computational complexity in establishing a narrow-band subliminal channel can be reduced, and the channel capacity can be increased with the help of memory [1]. NB-IoT features, connection analysis, latency analysis, and coverage augmentation strategies were examined, among other things. The distinctions between NB-IoT and other communication technologies have been emphasized.

The perception, transmission, and application layer security needs of NB-IoT were explored [2]. Secure communication is accomplished by PUF-based chip binding, where security is dependent on the PUF's inner circuit and the platform initialization procedure rather than on pre-distributed secret keys. If the chip is not detachable, the transmission remains confidential and secure. The PUF-based security enhancement provides end-to-end security, improved performance, and lower operational costs [3]. Security is crucial in LPWAN, as it is a wireless communication network that uses simple cryptography and is prone to a wide range of attacks. This paper discusses and evaluates LPWAN technologies LoRa, Sigfox, NB-IoT, and DASH7, as well as their network architecture and reliable communication mechanisms, from the perspective of IoT factors [4].

This research application aims to protect the structure from bandwidth spoofing, an attack based on a UAV-enabled Small Cell Access (SCA) device acting as an impediment between the user and a legitimate SCA, and to explore the case in which any barrier comes within the range of an NB-IoT capable device [5]. A security communication device is developed based on the narrowband Internet of Things (NB IoT) communication transmission system, which secures the data's authenticity, secrecy, and integrity. The security communication device has three components: an IoT platform, a key management distribution platform, and a secret key management distribution platform, all interconnected using the NB-IoT communication module [6]. Ad hoc networks are secured using a secure and customizable method.

This proposed system design integrates ECC and MAES to provide reasonable security and flexibility by detecting and preventing ad hoc network attacks using an intrusion detection system [7]. Sharmila et al. explored different types of adopted networks in mobile applications, including integrated ad hoc networks of various sizes and integrated ad hoc networks. Many advantages, applications, and problems of ad hoc networks regarding Quality of Service (QoS), power management, and security have been examined [8]. Thakur et al., in an information attack, the primary purpose is the information sent on the network, and in a controlled attack, the traffic in the network.

The research results were reviewed, and the best preventive measures were determined. This study precludes previous studies to clarify the biases associated with using MANET [9]. An analysis of rival narrowband Internet of Things (NB IoT) protocols, including Sigfox, LoRa, and 3GPP, is done to determine how well they manage security and privacy. The benchmark is based on a novel idea that combines the STRIDE threat model with a quick risk assessment to offer suggestions for mitigating high risk. Additionally, it has been demonstrated that moving on to a less demanding test can enhance the control performance of every NB IoT network protocol investigated in the survey [10].

A wireless MANET's security depends on routing. MANET routing flaws and dissecting the simple "black hole" issue approach that can be used to exploit them are studied. Point-to-point distance vector routing techniques are another issue tackled [11]. Technologies extensively used by the public are unlocked using techniques already present in military ad hoc networks. However, the military environment has additional requirements for communication and security solutions compared to the civilian environment. This paper suggests a security architecture for threatening settings for wireless ad hoc networks.

Special attention is devoted to malevolent management to guard against insider attacks on the network. Mobile wireless and NBIoT communication technologies are compared in terms of security, latency, availability, data transfer, power consumption, coverage and spectral efficiency. In addition, smart NB IoT applications such as smart homes and cities, smart services and environmental monitoring, and smart metering have been investigated. NB IoT security limitations that should be addressed immediately are listed [12]. Layering methods are used to provide a comparative assessment of security concerns. Many security attacks related to NB IoT have been studied, including node fault attacks, sharing attacks, synchronization attacks, battery attacks, and source code attacks [13].

This study aims to provide an overview of the discovery of MAC and physical processes and the architectural changes brought by the NB IoT standard. In addition, poll control of non-IP and IP packets from user planes and control planes and sending NB—IoT [14] is necessary. Refreshing ad hoc networks (multiple connections between nodes) adds new challenges and opportunities for protection against denial-of-service attacks.

A new cryptographic method called threshold cipher is used to provide security and to have important services that are the basis of security [15]. In the above cases, cryptography, encryption, and other routing protocols, such as AODV, provide security on only one level. Given enough time to decrypt the data, all the methods can be easily deciphered. Therefore, a security model has been developed using 3 levels.

3. Proposed Conceptual Model

A conceptual model was developed, and data was sent between the transmitter and receiver. The message to be sent is given 3 levels of security, and the data packet is formed and transmitted. The proposed model block diagram is shown in Figure 1. In the first level, the message bits are convoluted with a unique- receiver ID, and $Y_1[i]$ is formed. A unique ID is a code or identifier assigned to a specific entity or object in a system, database, or application to distinguish it from other entities or objects.

The uniqueness of an ID is typically ensured by using a combination of letters, numbers, and symbols and by limiting the length of the ID to a certain number of characters. The unique ID is assigned separately to each receiver. If the unique ID does not match, the data cannot be retrieved from the receiver side.

$$Y_1[i]=X[i]\otimes ID[i]$$

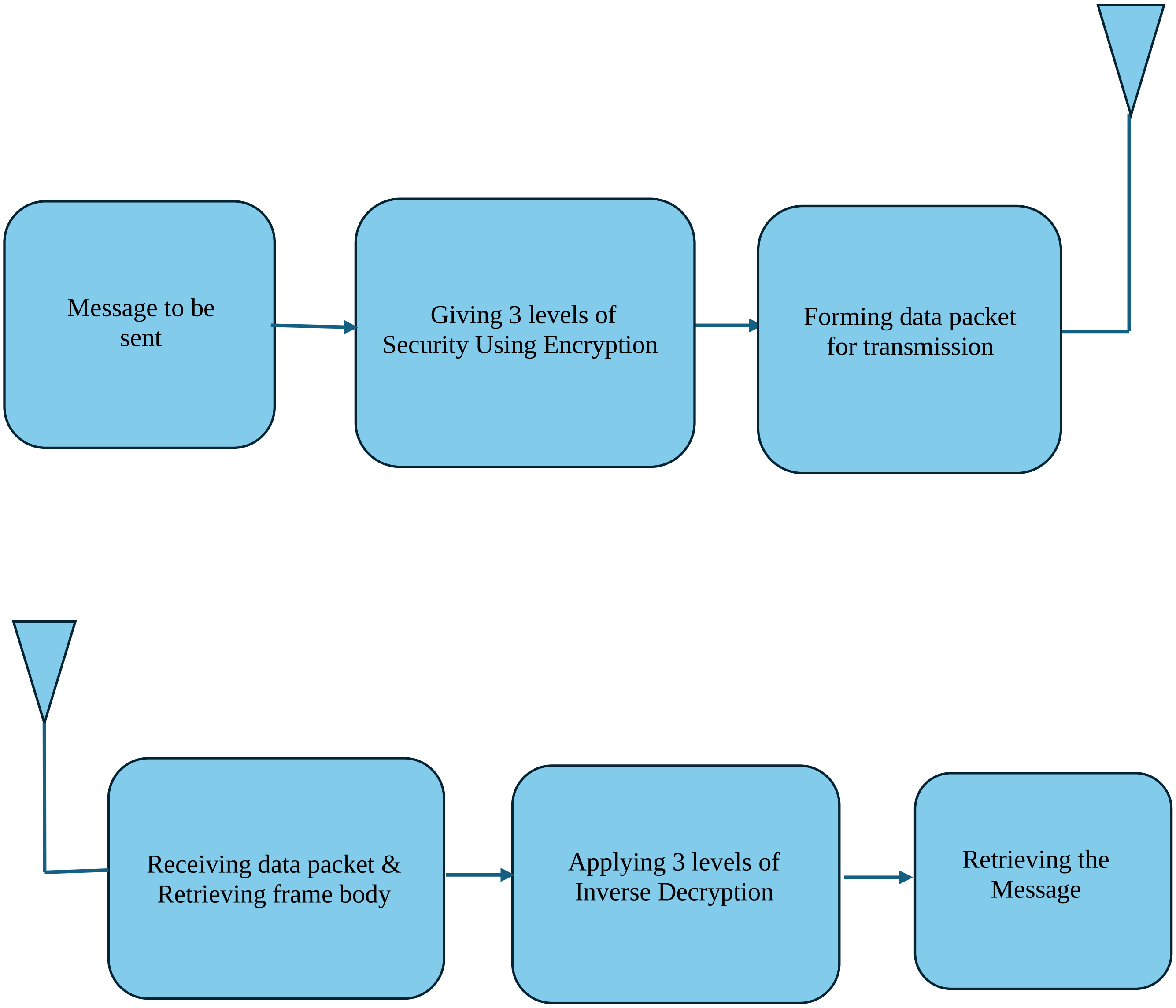

Message to be sent
Giving 3 levels of Security Using Encryption
Forming data packet for transmission
Receiving data packet & Retrieving frame body
Applying 3 levels of Inverse Decryption
Retrieving the Message

Fig. 1 Block diagram of encryption and decryption at transmitter and receiver, respectively

MAC Header	Frame Body	FCS

Fig. 2 Bandwidth allocation for 9 channels and 8 guard bands

In the second level, $Y_1[i]$ is convoluted with a random key using the date and the current time, and $Y_2[i]$ is formed. A random key is a cryptographic key that is generated using a random process. Cryptographic keys are used to encrypt, and decrypt data, and a random key is generated without any predictable pattern or sequence.

$$Y_2[i]=Y_1[i]\otimes K[i]$$

The third level of security is given by forming a polynomial equation $Y_3[i]$ using $Y_2[i]$.

$$Y_3[i]=4Y_2[i]+7$$

Formation of packet $Y_4[i]$ using $Y_3[i]$ as frame body as shown in Figure 2. Send $Y_4[i]$ packet for transmission. The above process of Encryption is explained in the form of a flow chart, as shown in Figure 3. On the Decryption side, $Y_4[i]$ is received.

In the first level of decryption, retrieve the $Y_3[i]$ frame body from the packet. Generate $Y_2[i]$ from inverse polynomial operations and then generate $Y_1[i]$ and $X[i]$ from deconvolution operations, respectively. The process of Decryption is explained in the form of a flow chart, as shown in Figure 4.

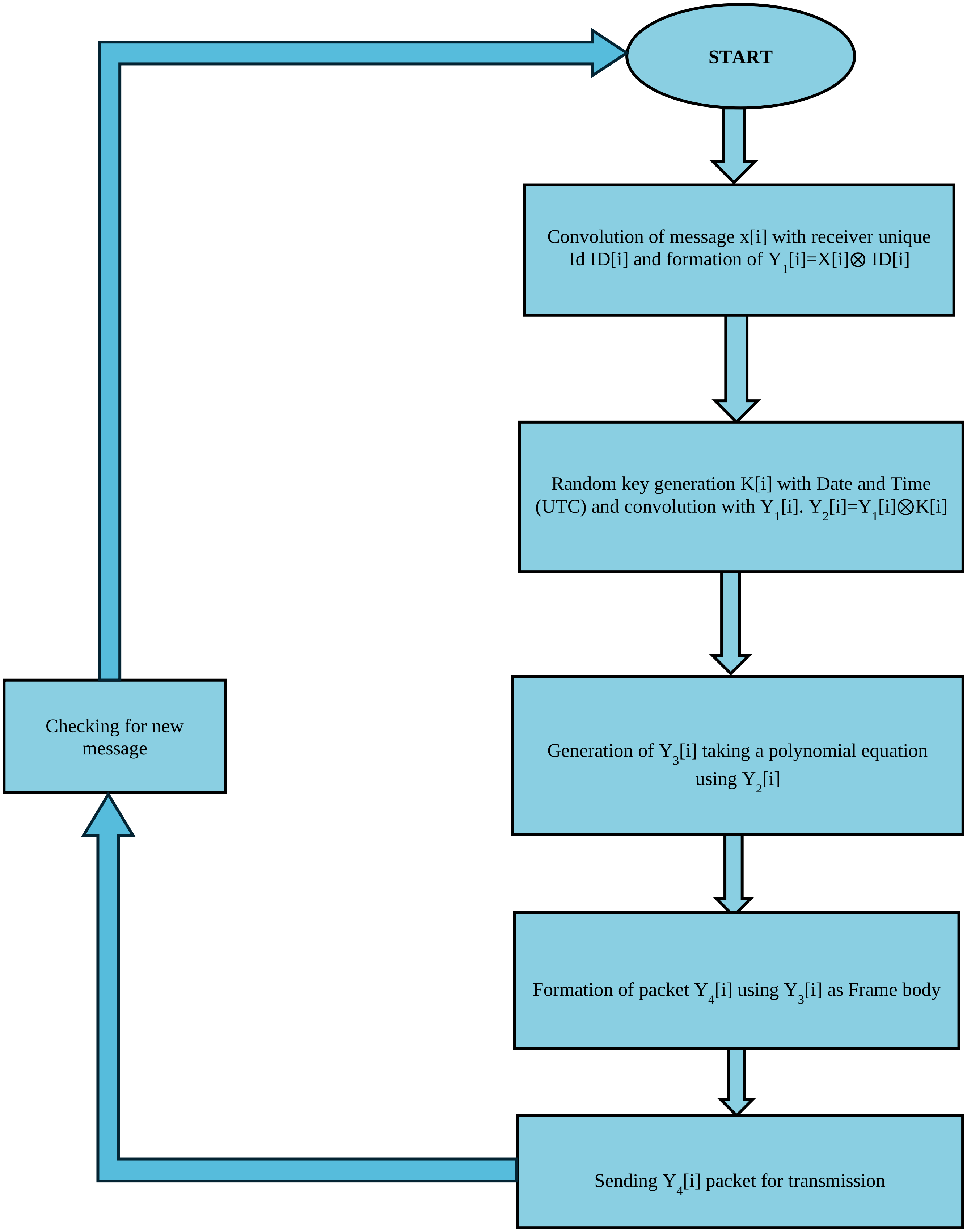

START
Convolution of message x[i] with receiver unique Id ID[i] and formation of $Y_1[i]=X[i]\otimes ID[i]$
Random key generation K[i] with Date and Time (UTC) and convolution with $Y_1[i]$. $Y_2[i]=Y_1[i]\otimes K[i]$
Generation of $Y_3[i]$ taking a polynomial equation using $Y_2[i]$
Formation of packet $Y_4[i]$ using $Y_3[i]$ as Frame body
Sending $Y_4[i]$ packet for transmission
Checking for new message

Fig. 3 Flowchart for data encryption at the transmitter

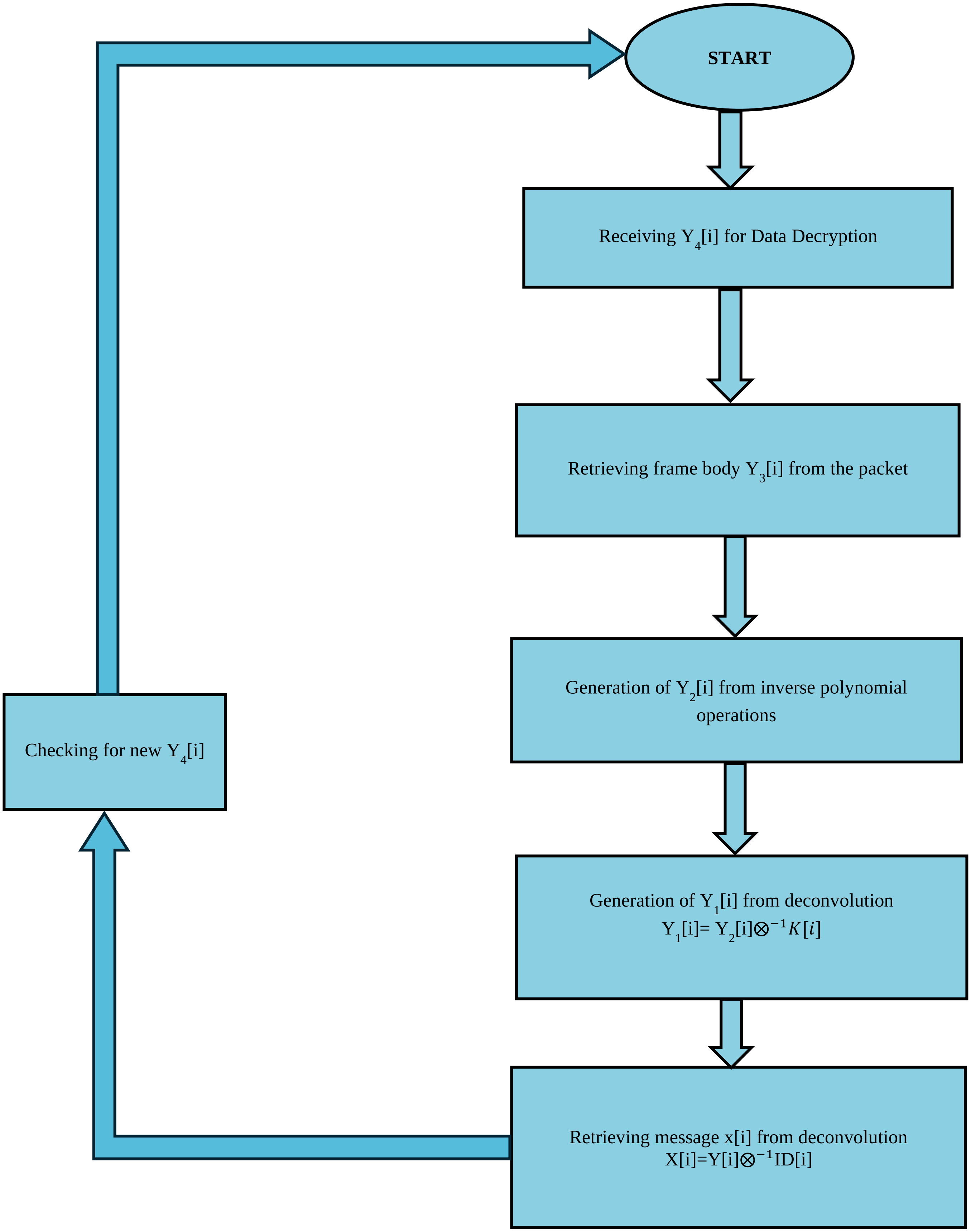
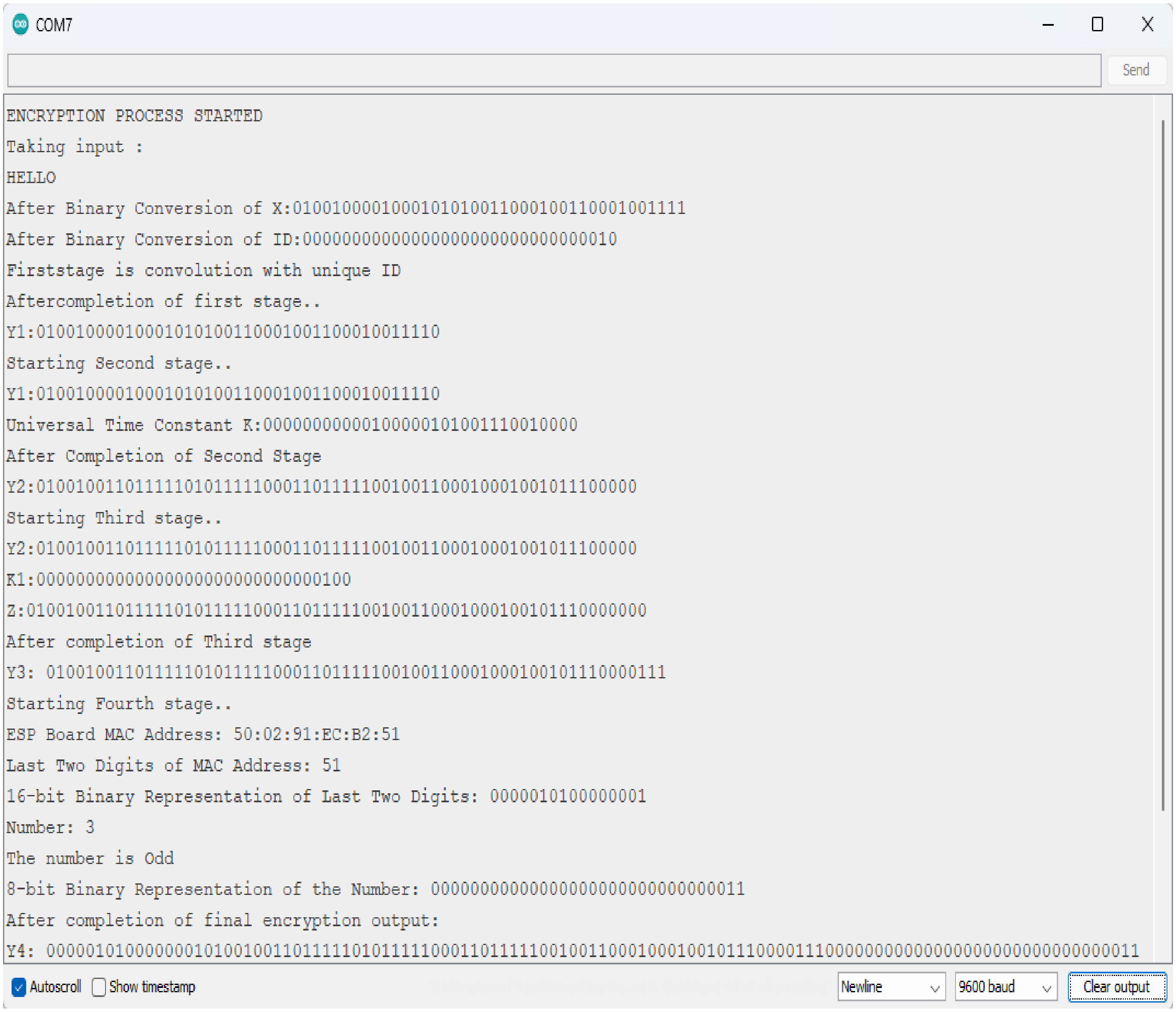

START
Receiving Y_4[i] for Data Decryption
Retrieving frame body Y_3[i] from the packet
Generation of Y_2[i] from inverse polynomial operations
Generation of Y_1[i] from deconvolution
$Y_1[i]= Y_2[i]\otimes^{-1}K[i]$
Retrieving message x[i] from deconvolution
$X[i]=Y[i]\otimes^{-1}ID[i]$
Checking for new Y_4[i]

Fig. 4 Flowchart for data decryption at receiver



```
ENCRYPTION PROCESS STARTED
Taking input :
HELLO
After Binary Conversion of X:0100100001000101010011000100110001001111
After Binary Conversion of ID:00000000000000000000000000000010
Firststage is convolution with unique ID
Aftercompletion of first stage..
Y1:0100100001000101010011000100110001001110
Starting Second stage..
Y1:0100100001000101010011000100110001001110
Universal Time Constant K:00000000000100000101001110010000
After Completion of Second Stage
Y2:0100100110111111010111111000110111111001001100010001001011100000
Starting Third stage..
Y2:0100100110111111010111111000110111111001001100010001001011100000
K1:00000000000000000000000000000100
Z:010010011011111101011111100011011111100100110001000100101110000000
After completion of Third stage
Y3: 010010011011111101011111100011011111100100110001000100101110000111
Starting Fourth stage..
ESP Board MAC Address: 50:02:91:EC:B2:51
Last Two Digits of MAC Address: 51
16-bit Binary Representation of Last Two Digits: 0000010100000001
Number: 3
The number is Odd
8-bit Binary Representation of the Number: 00000000000000000000000000000011
After completion of final encryption output:
Y4: 000001010000000101001001101111110101111110001101111110010011000100010010111000011100000000000000000000000000000011
```

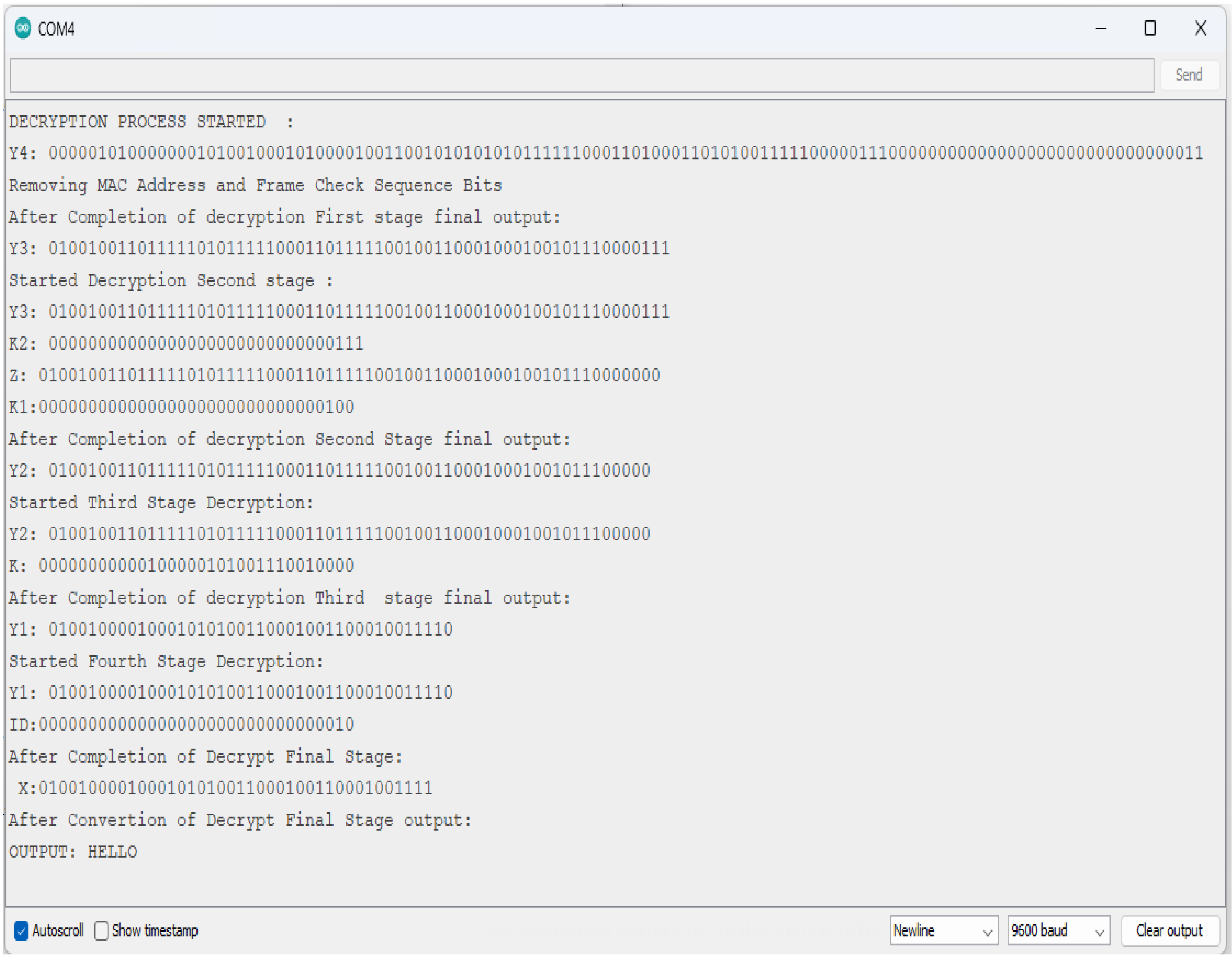
Fig. 5 Message to be sent encrypted in 3 levels and formation of data packet

4. Results

This process is used for transmitting tactical commands in Military applications. To demonstrate the process, a single message, “HELLO”, was considered. In the first level of encryption, each letter of input ‘HELLO’ is converted to a corresponding 8-bit binary representation, and the total 40 bits are convoluted, with the receiver's unique ID represented by 32 bits. The formed Y_1 is sent to the next stage. In the second stage, Y_1 is convoluted with a Universal Time Constant (K) represented by 32 bits, and the formed Y_2 is sent to the next stage. In the third stage, a polynomial equation Y_3 is formed and sent to the next stage by taking Y_2 and time constants A and B. The formed Y_3 forms a data packet Y_4 using MAC Header and Frame Check Sequence (FCS) bits and is sent for transmission. The data is Encrypted in 3 levels, as shown in Figure 5 and sent from the Transmitter to the Receiver.

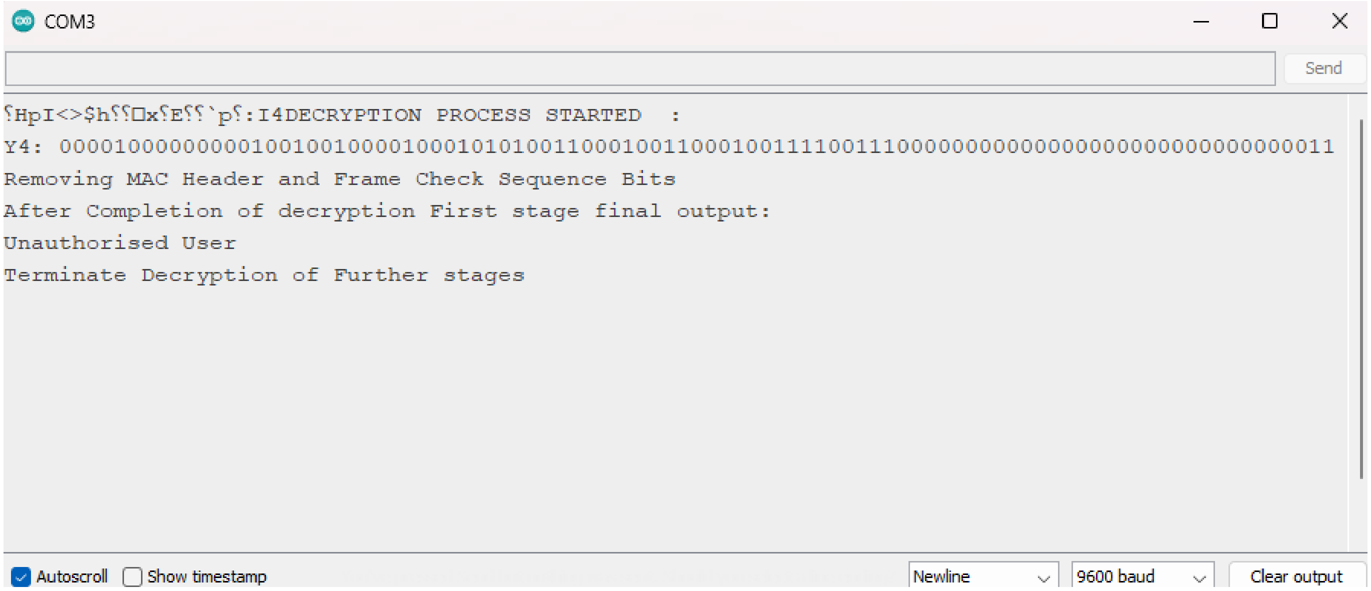
At the receiver, the first stage of the Decryption process will start by removing the MAC header and frame check sequence bits from Y_4 and Y_3 will be formed. In the second stage of Decryption, Y_2 is formed by subtracting the constant K2 from Y_3 and doing the inverse polynomial operations.

In the third stage of Decryption, Y_1 is formed from deconvolution of Y_2 with K (UTC). In the final stage of Decryption, message bits X are obtained by deconvoluting Y_1 with a unique ID. The data is decrypted in three levels, as shown in Figure 6, and the original message that was sent, “HELLO, “is retrieved. If the data packet is sent to an Unauthorized user, the MAC address of the unauthorized user will not match. The unauthorized user will not be able to retrieve the first stage output only, and the process is terminated, as shown in Figure 7.



```
DECRYPTION PROCESS STARTED  :
Y4: 000001010000000101001000101000010011001010101010111111000110100011010100111110000011100000000000000000000000000000011
Removing MAC Address and Frame Check Sequence Bits
After Completion of decryption First stage final output:
Y3: 0100100110111111010111110001101111100100110001000100101110000111
Started Decryption Second stage :
Y3: 0100100110111111010111110001101111100100110001000100101110000111
K2: 00000000000000000000000000000111
Z: 0100100110111111010111110001101111100100110001000100101110000000
K1:00000000000000000000000000000100
After Completion of decryption Second Stage final output:
Y2: 010010011011111101011111000110111110010011000100010010111100000
Started Third Stage Decryption:
Y2: 010010011011111101011111000110111110010011000100010010111100000
K: 00000000000100000101001110010000
After Completion of decryption Third  stage final output:
Y1: 01001000010001010100110001001100010011110
Started Fourth Stage Decryption:
Y1: 01001000010001010100110001001100010011110
ID:00000000000000000000000000000010
After Completion of Decrypt Final Stage:
 X:0100100001000101010011000100110001001111
After Convertion of Decrypt Final Stage output:
OUTPUT: HELLO
```

Fig. 6 Message decrypted in 3 levels and retrieving the original message "HELLO" at the receiver



```
ʕHpI<>$hʕʕ□xʕEʕʕ`pʕ:I4DECRYPTION PROCESS STARTED  :
Y4: 00001000000000100100100001000101010011000100110001001111001110000000000000000000000000000011
Removing MAC Header and Frame Check Sequence Bits
After Completion of decryption First stage final output:
Unauthorised User
Terminate Decryption of Further stages
```

Fig. 7 The Process of retrieving the original message at the unauthorized receiver is terminated

5. Conclusion

A secure conceptual model that was effective and efficient was developed. Data was securely transmitted from the transmitter to the receiver. A 3-level encryption algorithm is successfully implemented on the transmitter side, and the 3-level decryption is done on the receiver. It was also shown that data is not decrypted at the unintended receiver. When comparing the existing methodologies with the proposed method of secure communication between transmitter and receiver, it was clear that the sent secret message is securely transmitted to the authorized receiver, and any unauthorized receiver cannot decrypt the message. Even given enough time to decrypt the message, as the unintended receiver or the eavesdropper has no idea about the polynomial constants or the UTC, it is impossible to decrypt the secret message.

Future Scope

This work can be further extended to reduce the computational overhead in constructing the 3-level data Encryption and the delay in retrieving the original message after 3-level Decryption.

References

[1] Kazukuni Kobara, and Hideki Imai, “On The Channel Capacity of Narrow-Band Subliminal Channels,” *Proceedings International Conference on Information and Communications Security*, Springer, Berlin, Heidelberg, pp. 309-323, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[2] Min Chen et al., “Narrow Band Internet of Things,” *IEEE Access*, vol. 5, pp. 20557-20577, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yuesong Lin et al., “Research on PUF-Based Security Enhancement of Narrow-Band Internet of Things,” *Proceedings 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, Krakow, Poland, pp. 702-709, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[4] Smilty Chacko, and Deepu Job, “Security Mechanisms and Vulnerabilities in LPWAN,” *Proceedings International Conference on Recent Advancements and Effectual Researches in Engineering Science and Technology (RAEREST), IOP Conference Series: Materials Science and Engineering*, Kerala State, India, vol. 396, no. 1, pp. 1-8, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] Vinod Kumar et al., “Security Issues in Narrowband-IoT: Towards Green Communication,” *Proceedings 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 369-371, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Zhiqiang Cao, and Shuhua yang, “A Security Communication Device Based on Narrowband Internet of Things,” *Proceedings 2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, pp. 2141-2145, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Hiral Vegda, and Nimesh Modi, “Secure and Efficient Approach To Prevent Ad Hoc Network Attacks Using Intrusion Detection System,” *Proceedings 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp. 129-133, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] S. Sharmila, and T. Shanthi, “A Survey on Wireless Ad Hoc Network: Issues and Implementation,” *Proceedings 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, India, pp. 1-6, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sharat S Kariyannavar, Shreyas Thakur, and Aastha Maheshwari, “Security in Mobile ADHOC Networks: Survey,” *Proceedings 2021 6th International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, pp. 135-143, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Eric Yocam, “Narrow-band Internet of Things Protocol Standards: Survey of Security and Privacy Control Effectiveness,” *Proceedings 2020 International Symposium on Networks, Computers and Communications (ISNCC)*, Montreal, QC, Canada, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hongmei Deng, Wei Li, and D.P. Agrawal, “Routing Security In Wireless Ad Hoc Networks,” *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70-75, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[12] C. Candolin, and H. H. Kari, “A Security Architecture For Wireless Ad Hoc Networks,” *Proceedings MILCOM 2002*, Anaheim, CA, USA, vol. 2, pp. 1095-1100, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[13] Vinod Kumar, Rakesh Kumar Jha, and Sanjeev Jain, “NB-IoT Security: A Survey,” *Wireless Personal Communications*, vol. 113, no. 4, pp. 2661-2708, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Collins Burton Mwakwata et al., “Narrowband Internet Of Things (NB-IOT): From Physical (PHY) And Media Access Control (MAC) Layers Perspectives,” *Sensors*, vol. 19, no. 11, pp. 1-34, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[15] Lidong Zhou, and Z.J. Haas, “Securing Ad Hoc Networks,” *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999. [CrossRef] [Google Scholar] [Publisher Link]