PAPER NAME

Journal_Amil_Isminarti_Ardiaty_Syafaruddin

WORD COUNT

4302 Words

CHARACTER COUNT

21188 Characters

PAGE COUNT

11 Pages

FILE SIZE

650.7KB

SUBMISSION DATE

Jun 10, 2022 8:17 PM GMT+8

REPORT DATE

Jun 10, 2022 8:19 PM GMT+8

21% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 18% Internet database
- 20% Publications database
- Crossref database
- Crossref Posted Content database
- 0% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 25 words)

IMPROVED DATA SECURITY USING AES ALGORITHM ON LONG RANGE (LORA) COMMUNICATION SYSTEM AT SMART GRID

Isminarti[1,2], Amil Ahmad Ilham[3,*], Ardiaty Arief[1], Syafaruddin[1]
[1]Department of Electrical Engineering,
[3]Department of Informatics
Universitas Hasanuddin
Jl. Poros Malino KM.6 Bontomarannu (92127) Gowa
South Sulawesi, Indonesia
[2]Department of Mechatronic Engineering
Politeknik Bosowa
Makassar, Indonesia
http://eng.unhas.ac.id. E-mail: teknik@unhas.ac.id
* Corresponding author: amil@unhas.ac.id
isminarti@politeknikbosowa.ac.id;isminarti20d@student.unhas.ac.id;
syafaruddin@unhas.ac.id;ardiaty@eng.unhas.ac.id

Abstract – Research on data security on smart grids is the main focus of this research. The long-range (LoRa) communication system has developed and is equipped with a capable security system, but there are still many obstacles in the field that cause the need to increase data security in this communication system. The AES algorithm used in this study was added to improve data security on the sender and recipient sides through the encryption and decryption of messages. This research produces an encryption and decryption model using symmetric cryptographic block cipher type AES-256 which is then inserted into the modulation and demodulation process at the LoRa transmitter and receiver on the smart grid. The results of this study prove that by using the AES-256 block cipher, the security messages sent are layered and the results of the occupied bandwidth simulation show that the bandwidth used has suitable the ITU-R standard which is 99%.

Keywords – security, AES, ciphertext, communication, smart grid.

1. **Introduction.** A smart grid is a two-way communication network where the role of information is very important in the process of energy transmission and distribution. The smart grid is a combination of ICT with computer processing capabilities and electrical systems to improve communication between users. Smart grid constraints are when exposed to various malicious cyber attacks that can destroy basic infrastructure and disruption of communication between networks and users [1]. Cyber security systems can be created on the smart grid by authenticating authenticated users. A researcher authenticates a two-way smart meter between a smart meter on the customer side and a server on the PLN side. This study presents a key model (cryptography) with two-way authentication between smart meters and PLN and examines the LPWAN protocol architecture to evaluate cyber attack behavior on smart grids [2]. Other researchers have also investigated security issues in smart grids on the customer and electricity provider side and proposed a methodology to improve secure communication wherein his research

shows that, as the spurious factor increases, the detection time by the proposed algorithm increases [1]. A research community is also developing suitable analytical models that can play an important role in the study of smart grid technologies. and a mathematical model is proposed that accurately estimates the probability of success of LoRaWAN network packets on bidirectional traffic, i.e., uplink (UL) and downlink (DL) transmissions, and accounts for the most important features of LoRa chipsets and the LoRaWAN standard [3]. Lora can measure the reliability of a communication system from network performance where failure can be divided into two factors, namely intrinsic factors (hardware, software, communication protocols, etc.) and extrinsic (weather conditions, malicious agents, terrorist attacks, etc.) [4]. A researcher using the low latency minimized latency and collision-free multi-hop LoRa network protocol thus proposes a prototype LoRa node using the MultiTech mDot module, and the results show that the proposed protocol provides high reliability, and parallel transmission, minimized number of time slots defined. for all links in the network, minimized packet size and low latency [5]. Security research is also researched [6] by analyzing that LoRaWAN reduces communication power by setting different transmission latencies for different end devices, and AES does not take encryption strength into account, the AES encryption process results in lower power consumption of up to 26.2%. Other researchers also provide an overview of the AES algorithm and explain some of the important features of this algorithm in detail and demonstrate some previous research that has been done by comparing it with other algorithms such as DES, 3DES, Blowfish, etc. This research is not head to head because it compares with the old algorithm that since January 1997, the US National Institute of Standards and Technology (NIST) announced the start of an initiative to develop a new encryption standard namely AES and in 2002, its name was changed to Advanced Encryption Standard (AES) and published by NIST. The new encryption standard will become the Federal Information Processing Standard (FIPS), replacing the old Data Encryption Standard (DES) and triple-DES [7]. A researcher uses Sx1278 to send data in the form of small packets based on wide-area radio technology where the main problem from Lora Technology revealed in the study is the average packet loss when sending data is almost 50%, i.e. there is a 0.5 chance that packets will not be received at the receiving side and to improve the reliability and security of the data sent, the researcher proposes a basic logic to make sending and receiving packets more reliable using the concept of packet serialization and securing it using the AES algorithm [8].

The purpose of this study is to produce an encryption and decryption model using symmetric cryptography of the AES-256 block cipher type which is then inserted into the LoRa transceiver modulation and demodulation process on the smart grid to increase the reliability of the LoRa communication system. This research will contribute to the solutions previously researched by [1]–[3], [5], [6], [8]. The contribution of this research is to produce a LoRa communication system transceiver model on a smart grid using the AES-256 algorithm to improve data security on the transmitter and receiver side as a contribution to the communication system on the customer and electricity provider side which requires high constraints in maintaining data confidentiality.

2. **Data Security Systems.** The data security system is the main thing in maintaining the information/messages/data that will be conveyed. The communication network on the smart grid requires data security that is difficult for profit-seeking parties to hack, so to

maintain the security of data information conveyed by the transmitter to the receiver is safe against threats, a layered security level using cryptography is needed.

2.1. **Encryption and Decryption Process.** Cryptography is a method to protect data (encrypt and decrypt information) from intruders or to prevent unauthorized access when transferring data over an open channel network. The decryption process must be known by the sender and recipient. There are 2 types of encryption in cryptography, namely symmetric key cryptography, and asymmetric key cryptography, symmetric-key cryptography will be discussed in this study. Symmetric key cryptography relies on a single key for the encryption and decryption of information. This key needs to be kept secret and the sender and recipient have the same key, which is different from asymmetric key cryptography which uses a different secret key so that it requires more processing time [9][10].

Encryption is the process of encoding data to prevent intruders from reading the original data easily. This stage can convert the original data (Plaintext) into an unreadable format known as Ciphertext. While decryption is the opposite of encryption. This is the process of converting ciphertext to original text without losing any words in the input text. The cryptographic process relies on mathematical calculations with substitutions and permutations with or without keys. Today, the network has an important role to transfer data accurately and quickly from source to destination. Data is not secure enough to be transferred strictly confidential. Information security has become one of the main challenges of sharing resources with data communication over computer networks.

DES (Data Encryption Standard) and AES are both symmetric block ciphers. DES has a smaller key size which makes it less secure to beat triple DES but is slower. The basic complexity between DES and AES is that in DES the plaintext square is isolated into two halves before the main computation starts while in AES the entire square is arranged to obtain the ciphertext. By examining a few more differences between DES and AES. DES is a more established computation and AES is computation driven which is faster and more secure than DES. AES (Advanced Encryption Standard) is an encryption-decryption algorithm for data. AES supports keys with lengths of 128, 192, and 256 bits. This cryptographic key is used to encrypt and decrypt data that is in blocks of length 128, 192, and 256 bits. AES was developed based on algebraic operations and multiple encryption cycles for communication security which was nominated by NIST as an algorithm that is capable of high computational efficiency and can be used in various applications, especially in high-speed broadband links.

TABLE 1. AES Features[9].

Features	**AES**
Block size (bits)	128
Key Size (bits)	128, 192, or 256
Matrix orientation	Input is mapped column-wise
Number of rounds	10,12, or 14
Key expansion	Dedicated expansion algorithm
GF(28 Polynomial	$x^8+x^4+x^3+x+1$ (011B)
Origin of S-box	The multiplicative inverse in GF (2^8) plus affine transformation
Origin of round constants	Elements 2^i of GF (2^8)

Features	AES
Diffusion layer	Left multiplication by 4x4 circular MDS matrix (2,3,1,1) – mix columns
Permutations	Shift rows

AES consists of 3 block ciphers namely AES-128, AES-192 and AES-256 [11], [12]. Figure 1 below is the basic structure of AES:

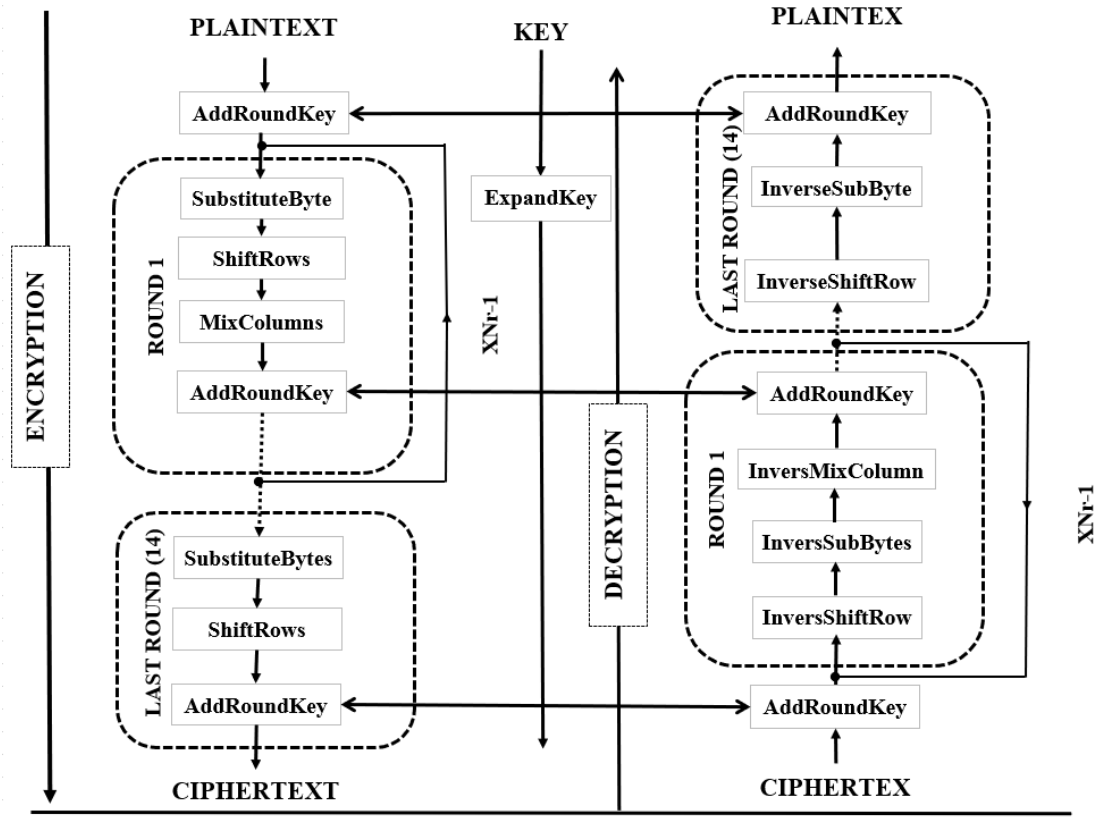


FIGURE 1. Basic Structure of AES[13], [14].

Parameters, symbols, and algorithm functions as shown in Figure 1 above are described below:

1. The plaintext is input data or messages in the form of text to the cipher or output from the inverse cipher which will be sent from the transmitter through the encryption process and to the receiver through the decryption process so that the input data received is the same as the output data or plaintext.
2. AddRoundKey() is a Transformation in Cipher in the encryption process and InverseCipher in the decryption process where RoundKey is added using XOR operation. The length of the RoundKey is equal to the size of the State, in this study we use the value Nb = 4 so that the length of the RoundKey is equal to 128 bits/16 bytes [12]. Nb is the number of columns (32-bit words) as shown in Table 2 below:

TABLE 2. Block cipher round combination

Block Cipher	KeyLength (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES-128	4	4	10

Block Cipher	KeyLength (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES-192	6	4	12
AES-256	8	4	14

In this study, we used the AES-256 block cipher with Nk=8, Nb=4, and Nr=14.

3. SubstituteByte() is a non-linear byte substitution that operates independently on each byte State using a substitution table (S-box). Tables 3 and 4 below are S-box tables, namely non-linear substitution tables used in several byte substitution transformations in encryption and decryption:

TABLE 3. Substitution Table (S-Box) at encryption process[10]–[12].

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	IE	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

The byte substitution process is carried out to modify the data in a nonlinear way to hide the relationship between the original and the encrypted message.

TABLE 4. Inverse substitution Table (Inverse S-Box) at decryption process [11].

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

4. ShiftRow() is the process of shifting rows from one another to increase the complexity of the algorithm, in this process, the first row is skipped, the second row is moved to one place, the third row is moved to two places and the last row is moved three places. ShiftRow is done in the encryption process while in the decryption process it is called InversShiftRows. Row shifting and column mixing will result in random data.
5. MixColumns() is a vertical random process so that with byte transposition, the encryption process is much more complicated so that the encryption results are very sophisticated and difficult to hack unless someone has a secret key.

AES algorithm made using the FIBS-197 standard. This algorithm is not built for speed and does not hide text messages. The function executes AES256 based on the key size. The function also doesn't check if the key or input size is the correct length and will error if it's not the correct size.

2.2. **Modulation and Demodulation Process.** Spread spectrum LoRa is a patented modulation developed by Semtech (https://www.semtech.com/) based on chirp spread spectrum (CSS) modulation. LoRa modulation is often referred to as "chirp modulation"[15]. LoRa (Long Range) provides long-distance and low power consumption, low data rate, and data transmission security. On public, private, or hybrid networks, LoRa can be used to achieve more comprehensive coverage than cellular networks. LoRa technology can easily integrate with existing networks and enable low-power battery-operated Internet of Things (IoT) applications. LoRa uses radio signals where these signals carry no information other than a transmitter that is constantly on. The signal must be modified in some way to convey information. several ways can be done; two of the most popular methods are to alter the amplitude and the frequency [16]. CSS was developed for radar applications in the 1940s and used in military and aerospace communications. LoRa offers a trade-off between sensitivity and data rate while operating on fixed bandwidth channels of 125 kHz (for uplink channels) and 500 kHz (for downlink channels). In addition, LoRa uses an orthogonal dispersion factor. This higher spread factor provides increased processing gain and higher reception sensitivity [8].

In the demodulation process resampling can be done to balance the data, that is, draw a sample from some of the available data. Sampling is divided into two, namely undersampling and oversampling. The oversampling technique takes the minority class so that the proportion in the sample is greater than the original proportion.

3. **Proposed Method.** In this study, we insert an encryption process at the LoRa transmitter to improve data security at the transmitter and also the decryption process at the receiver side. The method used in this research is comparative, namely comparing the process of modulation and demodulation with and without security to improve data security with a high level of reliability. In this study, the researchers tried to encrypt using a plaintext transposition cipher as follows: "MODELING AND SIMULATION OF LONG RANGE (LORA) COMMUNICATION SYSTEM ON SMART GRID" the number of columns in the plaintext is 79 so it uses a 4X4 matrix, so the text will be filled in first automatically. row using 4X4 matrices as shown in Figure 2 below:

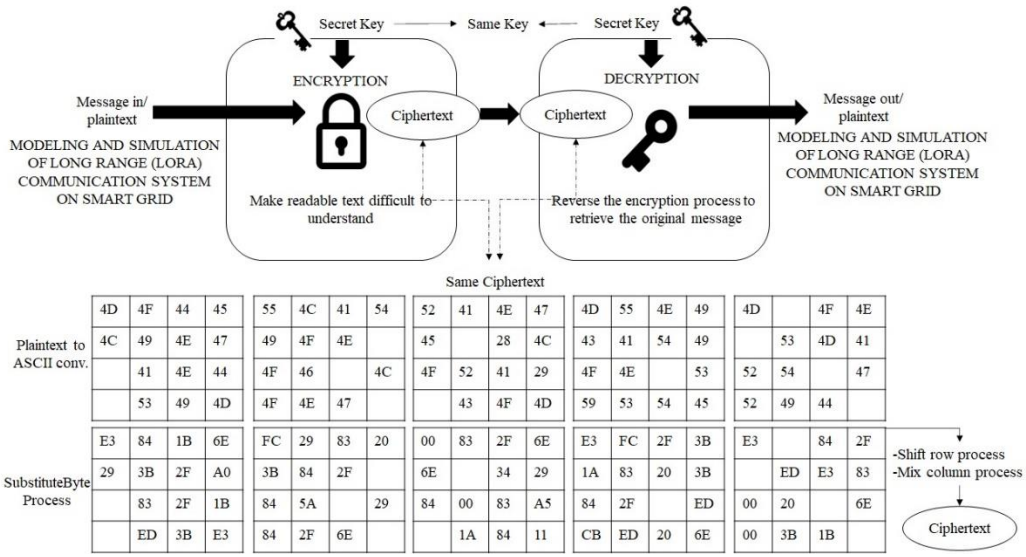


FIGURE 2. Encryption and decryption process on symmetric keys cryptography

After the first stage, which is converting plaintext into ASCII code as shown in the picture, then the next stage is substitute byte, shift row, mix column, and then add round key up to 14 rounds. This process then produces ciphertext which is processed at the transmitter and then the ciphertext and secret key received at the receiver are processed at the receiver until it produces the same plaintext as the information/message sent. The process of encryption and decryption at the transmitter and receiver can be seen in Figure 3 below which has been equipped with an encryption process. :

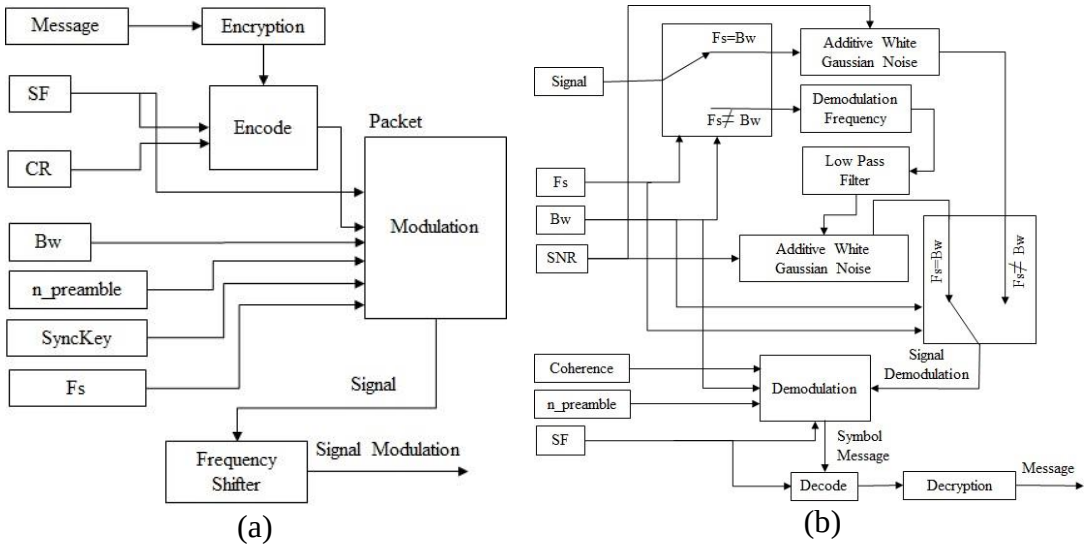


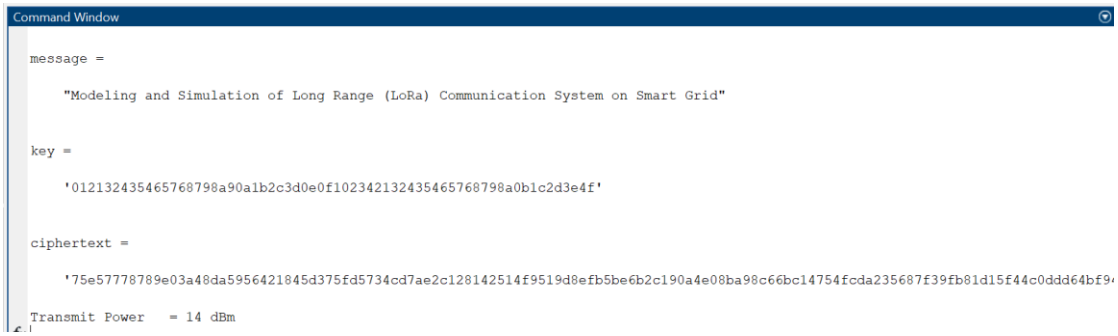
FIGURE 3. Secure data signal (a). Modulation on LoRa transmitter, (b). Demodulation on LoRa receiver

The block diagram above is a signal modulation process on the receiving side tested and validated using Matlab with good results according to the information sent. The node on the receiver will receive data from the transmitter and recap the RSSI and SNR. If the value of Fs = Bw, then the process will be carried out on AWGN, and if not, it will be forwarded to the frequency modulation process using MFSK and then filtered using LPF. Signal interference or interference in overlapping bands distorts so that AWGN processes the following procedure. This study will be tested by sending data messages with several

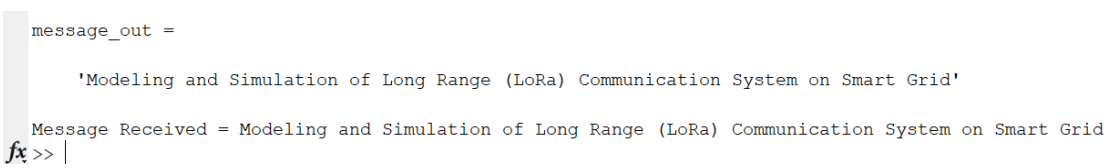
iterations to see the system's reliability [18]. Either unlicensed spectrum causes AWGN and fading interference. This is because of the various technologies that are not limited to LoRa. Radio spectrum congestion is correlated with population density, and it is essential to measure it, especially in urban environments. It has also been demonstrated that spectrum availability varies spatially and temporally.

Thus, the impact of interference cannot be abstracted into a single parameter but needs to be modeled statistically or can be regenerated based on empirical measurements. To incorporate Spatio-temporal interference, the proposed framework allows the injection of whole spectrum measurements as previously recorded by SDR. Thus, the SDR can be configured to capture the radio spectrum near the expected gateway location. The emulated LoRa frames are then linearly summed with the collected measurements. The resulting signal is then forwarded to the LE-Rx to demodulate and decode the LoRa signal. LoRa demodulated its signal below 19.5 dB of the noise floor. in contrast, One of the significant channel interferences in unlicensed spectrums is interference. Various technologies not limited to LoRa or even IoT compete for scarce resources. Radio spectrum congestion is correlated with population density, and it is essential to measure it, especially in urban environments. It has also been shown that spectrum availability varies spatially and temporally [19]. Therefore, the impact of interference cannot simply be abstracted into a single parameter such as an average but needs to be modeled statistically or regenerated based on empirical measurements. Thus, the SDR can be configured to capture the radio spectrum near the expected gateway location. Supposedly there is significant interference variability throughout the day. In that case, it is essential to collect interference measurements and sample this variability over different periods, then run the emulator during those periods.

4. **Simulation Result and Discussion**. This research produces a simulation of sending data packets by encrypting and decrypting messages that are authenticated with a secret key. Figure 4 below shows that this study succeeded in simulating messages with a high level of security.



(a)

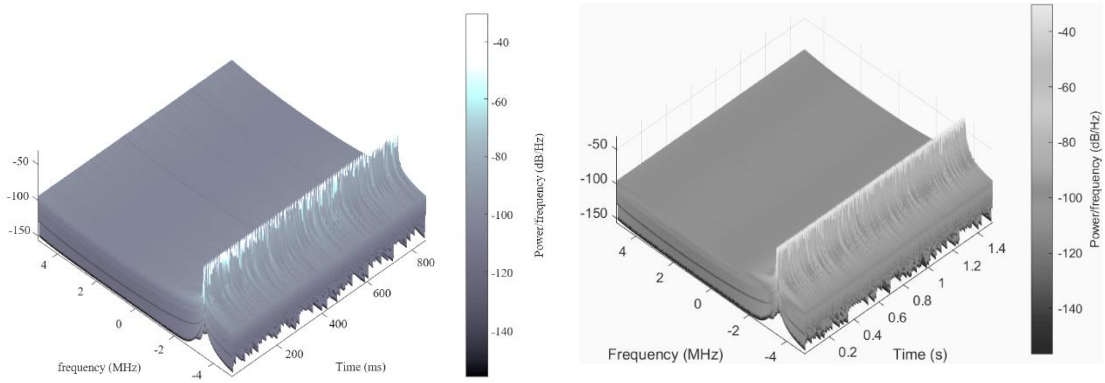


(b)

FIGURE 4. Simulation results of encryption and decryption of messages. (a) Simulation of the encryption process, (b) Simulation of the decryption process.

In Figure 5 below, the difference in spectrogram time is getting closer, indicating that the data sent is very long because it goes through a layered authentication process so it

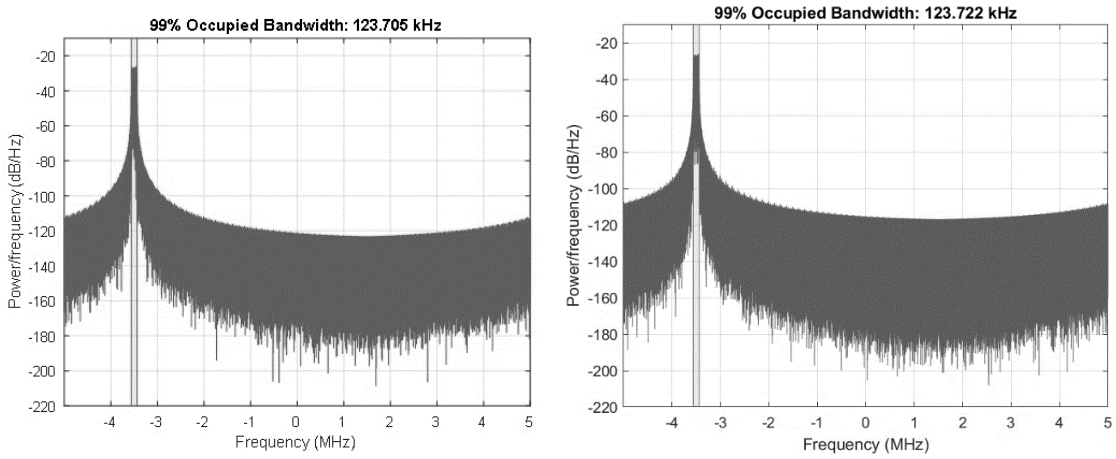
takes twice as long as the transmission process without encryption. The LoRa packet transmission spectrogram with 14 dBm of power and 99% occupied bandwidth indicates that the bandwidth used has complied with ITU-R standards [20] .



(a) (b)

FIGURE 5. The spectrogram on LoRa packet transmission with 14 dBm power (a). Without security (b). With AES-256 security.

In Figure 6 the width of the occupied bandwidth is also under the standards set for equipment in several areas, such as Japan and the United States. Where ITU-R defines it as the maximum bandwidth, excluding emissions that do not exceed a certain percentage of total emissions.



(a) (b)

FIGURE 6. Width of occupied bandwidth (a). Without security, (b). with security

5. **Conclusion.** The results of this study prove that by using the AES-256 block cipher the messages sent are layered security and noise reduction in the message sending process with and without security remains the same on the occupied bandwidth with 99% accuracy, which changes only when the LoRa packet spectrogram is getting longer because this algorithm is not made to generate speed and text messages can also be displayed because it is not hidden, nor does it check whether the key or input size is long or short which is clear as long as the secret key is not detected then the data will be gated.

Acknowledgments. This work is partially supported by the Indonesian Ministry of Education, Research, and Technology through the PDD grant.

REFERENCES

[1] T. Chen, X. Yin, and G. Wang, “Securing communications between smart grids and real users; providing a methodology based on user authentication,” *Energy Reports*, vol. 7, pp. 8042–8050, 2021.

[2] I. Studies and A. Panagi, “Exploring Communication Features and Security Vulnerabilities of Long-Range (LoRa) Networks,” no. May, 2021.

[3] M. Capuzzo, D. Magrin, and A. Zanella, “Mathematical Modeling of LoRa WAN Performance with Bi-directional Traffic,” *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.*, pp. 206–212, 2018.

[4] J. P. Astudillo León and L. J. de la Cruz Llopis, “Emergency aware congestion control for smart grid neighborhood area networks,” *Ad Hoc Networks*, vol. 93, p. 101898, 2019.

[5] D. L. Mai and M. K. Kim, “Multi-hop LOra network protocol with minimized latency,” *Energies*, vol. 16, no. 3, 2020.

[6] K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, Y. L. Huang, and C. H. Tsai, “AES-128 based secure low power communication for LoRaWAN IoT environments,” *IEEE Access*, vol. 6, pp. 45325–45334, 2018.

[7] V. F. Dr. Vladimir, *The Design of Rijndael*, vol. 1, no. 69. Printed in Germany: © Springer-Verlag Berlin Heidelberg 2002, 2001.

[8] A. Madaan, S. Bansal, A. Sahu, and F. Kidwai, “Peer to Peer Communication in GUI interface using Lora Technology,” *Procedia Comput. Sci.*, vol. 173, no. 2019, pp. 299–304, 2020.

[9] N. Mavrogiannopoulos, *Secure communications protocols and the protection of cryptographic keys*, no. June. 2013.

[10] W. Stalling, *Cryptography and Network Security*, Fourth. 2012.

[11] V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan, and A. A. S. Remya, “Implementation of Aes Algorithm on Text and Image.Pdf,” *2019 3rd Int. Conf. Trends Electron. Informatics*, no. Icoei, pp. 1279–1283, 2019.

[12] National Institute of Standards and Technology, *197: Announcing the advanced encryption standard (AES)*, vol. 2009. 2001.

[13] A. Singh, P. Agarwal, and M. Chand, “Analysis of Development of Dynamic S-Box Generation,” *Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 154–163, 2017.

[14] A. Muhammad Abdullah and A. Muhamad Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt,” no. June, 2017.

[15] L. Vangelista, “Frequency Shift Chirp Modulation: The LoRa Modulation,” *IEEE Signal Process. Lett.*, vol. 24, no. 12, pp. 1818–1821, 2017.

[16] P. Seneviratne, *Begining LoRa Radio Networks with Arduino*. 2019.

[17] Semtech, “LoRa and LoRaWAN: Technical overview | DEVELOPER PORTAL,” no. December 2019, p. 22, 2019.

[18] U. Noreen, E. Ahcenebounceuruniv-brestfr, and L. Clavier, “A Study of LoRa Low Power and Wide Area Network Technology,” *2020 Int. Conf. Adv. Technol. Signal Image Process. ATSIP 2020*, 2020.

[19] B. Al Homssi, K. Dakic, S. Maselli, H. Wolf, S. Kandeepan, and A. Al-Hourani, “IoT Network Design Using Open-Source LoRa Coverage Emulator,” *IEEE Access*, vol. 9, pp. 53636–53646, 2021.

[20] I. Sm, *RECOMMENDATION ITU-R SM.328-10 SPECTRA AND BANDWIDTH OF EMISSIONS*.

1999.

21% Overall Similarity

Top sources found in the following databases:

- 18% Internet database
- Crossref database
- 0% Submitted Works database
- 20% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Furht, Borko, Daniel Socek, and Ahmet Eskicioglu. "Fundamentals of M... Crossref	7%
2	cryptographyacademy.com Internet	6%
3	Bassel Al Homssi, Kosta Dakic, Simon Maselli, Hans Wolf, Sithampara... Crossref	2%
4	Bassel Al Homssi, Kosta Dakic, Simon Maselli, Hans Wolf, Sithampara... Crossref	1%
5	bu.edu.eg Internet	1%
6	csd.uwo.ca Internet	<1%
7	researchgate.net Internet	<1%
8	link.springer.com Internet	<1%

9 lora-developers.semtech.com

Internet

<1%