DOI: https://doi.org/10.57233/ijsgs.v10i2.640 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL10 (2) WEBSITE: https://fugus-ijsgs.com.ng

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY
(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

A New Lightweight Cryptographic Cipher for Detection and Prevention of Replay Attacks in Wireless Sensor Networks

[*1]Ibrahim Abubakar, [2]Muhammad Sani, [3]Yusuf Surajo

[*1] Computer Science Department, Federal University, Gusau, Nigeria
[2]Department of Statistics, Federal University Dutsin-ma, Katsina, Nigeria.
[3]Computer Science Department, Federal University Dutsin-ma, Katsina, Nigeria

Corresponding Author's Email: ibrahimabubakar958@gmail.com

Received on: April, 2024 **Revised and Accepted on:** May, 2024 **Published on:** July, 2024

ABSTRACT

Security concerns have been brought up by the electronics industry's widespread use of ubiquitous gadgets. The limitations of power consumption, space, and speed make it impractical to construct a full-fledged cryptographic environment using traditional encryption techniques in embedded systems like the Internet of Things. Lightweight cryptography is the main focus in order to get over these obstacles. This study proposes a new lightweight cryptography cipher that modifies the original PRESENT cipher by introducing a new layer between the S-box layer and P-layer of the current encryption-decryption process, lowering the encryption round, and changing the Key Register updating technique. The delta value function of the lightweight cipher known as the Modified Tiny Encryption Algorithm (MTEA) is added to the key register to update its encryption value. By adding an additional layer, we are able to lower the PRESENT round from 31 to 25, which is the bare requirement for security. Encrypting the key register increases the suggested algorithm's efficiency. By using MATLAB2022a and SIMULINK2022a are product of math work, widely used for mathematical computing algorithm development, data analysis, visualization and simulation.

Keywords: New lightweight cryptography cipher, NLCC Security, MTEA, LSA.

1. INTRODUCTION

These days, the popularity of wireless sensor networks (WSNs) and their many application fields is growing due to their low cost, flexibility, ease of deployment, and capacity for self-organization (Rawat *et al*., 2014). In a wireless sensor network (WSN), sensor nodes gather relevant environmental data (such as: temperature, humidity, and image quality) and send messages to the base station (BS) via wireless and multi-hop communications. As seen in figure 1, the BS is a downstream of all data originating from the sensor nodes.

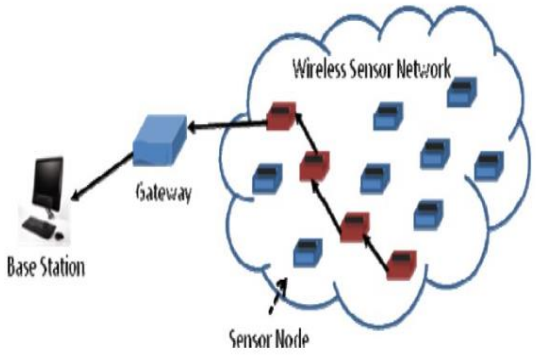

Figure 1: WSN Architecture

In many applications, including healthcare systems, intelligent agriculture, battlefield monitoring, home and industrial automation, and real-time reporting and response, WSN offer significant benefits. These applications result in significantly higher service quality. WSN integration with the Internet has received a lot of attention lately (Gubbi *et al*, 2013). WSNs are vulnerable to a variety of attack types that target various network levels. Due to various limitations (such as haphazard deployment in unmonitored areas) and restrictions on energy, computing, and storage resources, adopting strong and intricate security measures is extremely difficult when it comes to sensor network security (Saleem *et al*, 2023).

One of the most damaging attacks known to target the originality attribute of network messages is the replay (man-in-the-middle) technique. Typically, the attacker only replays the application data and signalling information many times, which can result in missing or erroneous alarms depending on how the message is repeated. In fact, the attacker might be more cunning and replay the message's data field alone. In wireless sensor networks, where sensed data is frequently sensitive and must be unique, as shown in Figure 1, this novel repeat attack scenario is far riskier.

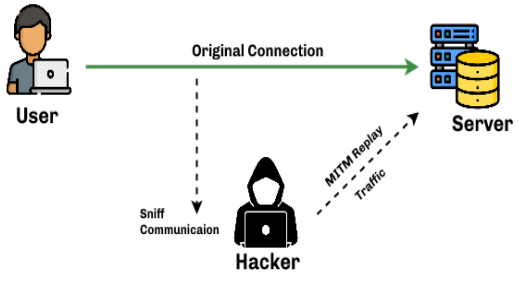

Figure 2: Replay Attack

A number of studies, have been carried out to prevent replay attacks in WSNs. In general, the cryptographic solutions are the emphasis of these publications. It is appropriate to use cryptographic techniques to improve WSN security (Jha *et al*, 2019; Khair *et al*, 2016). It would be challenging to implement fully functional cryptographic algorithms in sensor nodes due to limitations in computing time, resource efficiency, energy consumption, and security. This dissertation proposes a new lightweight cryptographic cypher to address the aforementioned issues. It does this by reducing the encryption round, altering the Key Register updating technique, and adding a new layer between the S-box layer and P-layer of the current encryption decryption process. The modified lightweight PRESENT cypher was proposed by Chatterjee and Chakrabort in 2020. In order to properly identify and avoid replay attacks in WSN, the new proposed cypher will use Modified TEA (MTEA) (Leon *et al*, 2019), as opposed to the Modified PRESENT cypher, which uses the TEA algorithm for updating the key register.

2. RELATED WORKS

Numerous studies have been carried out on cryptographic methods to safeguard users' data during the wireless sensor network (WSN) data transfer process. (Tripathy *et al*, 2021) introduced the Hybrid Encryption Technique (HET), a novel method that examines the attainment of data security in sensor networks using both two-key and single encryption. The Elliptic Curve Cryptography (ECC) technique is a sophisticated encoding method that is used in the HET approach to reduce the amount of the ciphertext. The Lempel-Ziv-Welch (LZW) compression technique is used to compress the data. The HET approach assures data security by protecting security primitives like integrity, confidentiality, and authentication. The method uses very little power and takes very little time for encryption and decryption.

Additionally, (Sachin *et al*, 2020) combined symmetric and asymmetric algorithms to create a novel hybrid encoding method that offers excellent security with less key management. Asymmetric and symmetric cryptography techniques are combined in the newly proposed hybrid resilient encryption method. The effective method for preventing clone node assaults on wireless sensor network communication that has been suggested. The hybrid technique makes use of hash algorithms for Message Digest 5 (MD5) and sophisticated cryptography standards including Dual Rivest-Shamir-Adleman (RSA), Byte-oriented Substitution-Permutation Network (BSDN), and Advances Encryption Standard (AES). The technology performs better than its competitors in terms of encryption and decryption time, but it consumes a lot of power and is susceptible to other attacks, according to the data.

A lightweight hybrid cryptographic system for WSNs called the Modified Playfair Cypher (AMPC) and AES were proposed by Anwar and Maha (Anwar and Maha, 2020). It was suggested that AMPC improve WSN security by using two cryptographic algorithms, modified PlayFair and AES, for data security and the first method, Diffie-Hellman, to secure the key exchange process. Despite increased protection, there was a noticeable increase in power consumption. However, because LSA uses a finite number of rounds and each round uses a unique key to ensure security, the suggested algorithm will use less power when transmitting data.

Additionally, a modified lightweight PRESENT cypher was proposed by Chatterjee and Chakrabort (2020). This cypher differs from the original PRESENT cypher (Bogdanov *et al*, 2007) in that it adds a new layer between the S-box layer and P-layer of the current encryption decryption process, reduces the encryption round, and modifies the Key Register updating technique. The Tiny Encryption Algorithm, or TEA, cypher is used to update the key register. The PRESENT round is lowered from 31 to 25 in the modified PRESENT technique to increase processing power and enhance performance. The suggested algorithm demonstrates its advantages over current lightweight cryptography methods. However, according to Adriaanse *et al*. (2021) TEA is vulnerable to equivalent key and related key attacks.

Additionally, a novel Lightweight Hybrid Cryptography (LWHC) was constructed by Prakash *et al*. (2019). This LWHC combines the Speck compact key scheduling technique with the PRESENT cypher and Lightweight Encryption Device (LED) cypher. The PRESENT, RECTANGLE, and LED S-Boxes are utilised to encrypt data. Using a 64-bit plain text as input, the method encrypts plain data and executes an XOR operation with a 128-bit scheduling key. The LED encryption method uses the conventional key technique, which is vulnerable to key attacks; in contrast, the LWHC makes use of the 128-bit key scheduling methodology, which makes it lightweight and secure against various key-related attacks. This updated method makes use of 128-bit keys that XOR with the 64-bit plain-text block to guarantee

Yue *et al*, 2019 integrated the qualities of high encoding efficiency of symmetric encryption techniques and high encoding intensity of asymmetric encryption techniques to propose a new hybrid encryption algorithm based on wireless sensor networks after analysing the security vulnerabilities of WSNs. Using the ECC asymmetric encryption technique and the AES symmetric encryption

DOI: https://doi.org/10.57233/ijsgs.v10i2.640 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL10 (2) WEBSITE: https://fugus-ijsgs.com.ng

algorithm, this technique first encodes the plaintext blocks. It then uses data compression to obtain the cypher blocks. Finally, it connects the Media Access Control (MAC) address and the AES key encoded through ECC to form the complete ciphertext message. The technique can reduce the total running time complexity, decryption time, and encryption time without compromising security, as shown by the results of its description and implementation.

Additionally, the Hamming Residue Method (HRM) was suggested by (Alotaibi, 2019) as a defence against hostile attacks on WSNs. Given the unreliability of the wireless network, the HRM was suggested as a means of preventing unauthorised parties from jeopardising the secrecy of the data. Hamming codes are used to identify and correct errors, therefore all communication systems are aware of these codes. Since WSNs are self-sufficient and energy-efficient, these codes can be employed to secure WSN networks without requiring additional infrastructure. Although the HRM approach increases the security of WSNs, it also consumes more power. Additionally, the computational complexity was overlooked, whereas the suggested hybrid solution will minimise power consumption and computational complexity by merely employing

The authors suggested a lightweight security technique that relies on Proxy Mobile Internet Protocol version 6 (PMIPv6) (Anandhavalli and Bhuvaneswari, 2019). The Diffie-Hellman authentication strategy that is integrated into the PMIPv6 protocol has been replaced with the suggested security authentication mechanism for WSNs. Consequently, a modified MAC address-based session key initialization protocol and a seed-based random number session key mechanism are presented and assessed. Power usage was minimal and

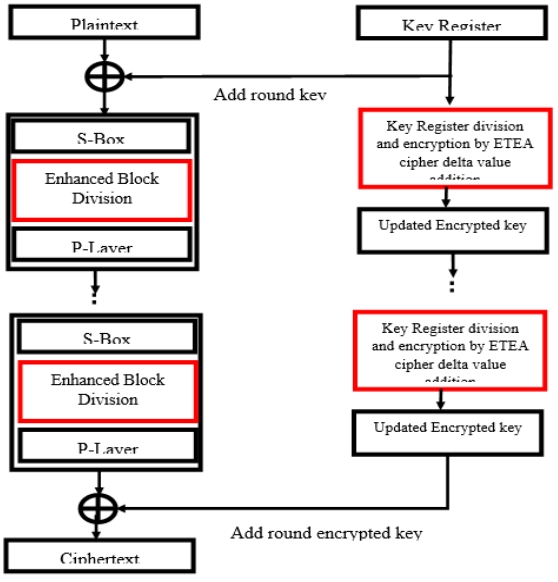

Figure 3: Block diagram of NLCC algorithm

production was subpar despite the reasonable level of protection.

Mahlake *et al*. (2022) developed a hybrid Lightweight Security Algorithm (LSA) that combines the Secure IoT (SIT) encryption technique with the Security Protocol for Sensor Networks (SPINS) to improve WSN data security while lowering the attack threshold and minimising power consumption in WSNs without compromising network performance. The simulation findings show that the suggested LSA technique outperformed the widely used Feistel and Substitution-Permutation Network (SPN) lightweight cryptography algorithms. Nevertheless, the SIT cryptographic cypher will perform poorly in terms of execution time and memory usage. The aim of this research work is to develop a new lightweight cryptographic cipher which uses the modified PRESENT cipher and MTEA algorithm so as to effectively detect and prevent replay attacks in WSN.

3. NEWLIGHTWEIGHT CRYPTOGRAPHIC CIPHER (NLCC)

A modified version of the PRESENT cypher (Thorat and Inamdar, 2018), one of the most well-liked lightweight algorithms and one that is frequently utilised in industries where the security of lightweight devices has been taken into consideration, is included in the proposed New Lightweight Cryptographic Cypher. The NLCC cypher that has been suggested is less intricate and more effective than the PRESENT cypher in terms of detection precision, power usage, data transfer rate, and overall latency. The proposed technique requires an 80-bit key and 64-bit textual input. Additionally, 64-bit encrypted text is produced. Fig. 3.2 shows the suggested algorithm's general structure. There are two components to the current PRESENT cipher's change. These two components increase the suggested algorithm's strength and efficiency significantly.

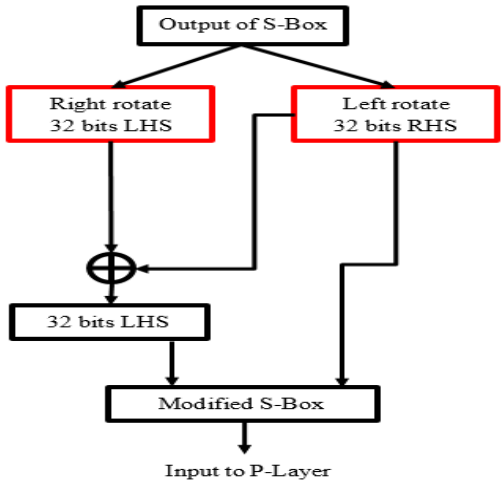

Figure 4: Block diagram of NLCC key register updating method

DOI: https://doi.org/10.57233/ijsgs.v10i2.640 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL10 (2) WEBSITE: https://fugus-ijsgs.com.ng

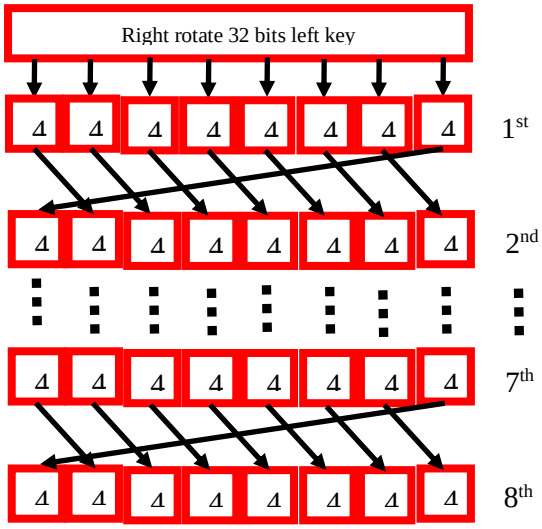

Figure 5: New Key Scheduling

3.1 NLCC Key Register Updating Method

The 64-bit round key (derived from the MSB position) in the original PRESENT cypher method is taken out of the 80-bit key register and applied to the XOR operation with the plaintext. The key register is then refreshed. This key register updating technique was altered by the suggested NLCC algorithm. The steps are detailed in Fig. 3.3. Initially, the 64-bit key that was taken out of the key register split into two 32-bit keys. Using a Delta value addition approach borrowed from the lightweight cypher TEA, the right half key begins at MSB and is encrypted (Shepherd, 2007). Nonetheless, TEA is vulnerable to related key assaults and equivalent key attacks. The NLCC algorithm suggested changing the subkeys of TEA (ETEA) on each round to increase security.

```
with ETEA Cipher Delta Value Addition*/
Function_KEY_Updating (KEY)
{
Repeat steps 1 to 5 10 times
1. Key_Left= Left_Half_Key[KEY];
2. Key_Left=Rotation_right (Key_Left, 8);
3. Key_Right= Right_Half_Key[KEY];
4. Key_Right=Rotation_left (Key_Right, 8
5. Encrypt_right_key_TEA Delta(Key_Right, ETEA_Key);
6. Key_Left ^ = Key_Right;
7. KEY =Merge (Key_Left, Key_Right); }
8. /*Updated KEY is now taken as an input to the next step*/
```

Figure 6: Pseudo code of NLCC Key Register Updating Algorithm

3.2 NLCC Extra Layer for Substitution-Box

Additionally, an additional layer is inserted between the S-Box layer and the Permutation Layer, altering the PRESENT encryption procedure. The S-box output was split into two 32-bit portions by the proposed NLCC cypher. The 32-bit left and right keys will be split into eight subkeys, each of which will be right-rotated eight times in the opposite scenario, as illustrated in Fig. 3. Subsequently, the left half is updated by XOR-ing the right component. Finally, combine the two halves to create a new combination of 64 bits. The procedure of decryption is identical to that of encryption; the rotation is done from left to right. The block diagram for the new layer is shown in Figure 7. The completed outcome fed into the subsequent Permutation layer. The two modifications increased the efficacy of the NLCC. There are 25 rounds in the NLCC.

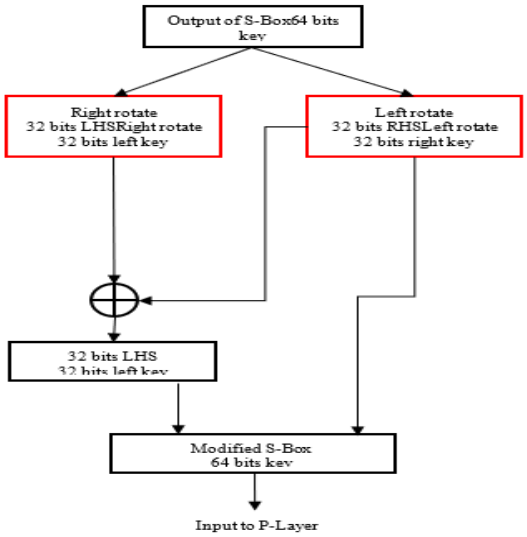

Figure 7: Block diagram of the new layer

```
/*Pseudo code of Stuffing Extra Layer In Between S-Box Layer and Player of
PRESENT Encryption */
Function _stuffing_layer(SBOX)
{
1. S_box_new[0] = LEFT[SBOX];
2. S_box_new[0] = Rotation_right (S_box_new[0], 8);
3. S_box_new[1] = RIGHT[SBOX];
4. S_box_new[1] = Rotation_right (S_box_new[1], 8);
5. S_box_new[0] ^ = S_box_new[1];
6. SBOX=Merge(S_box_new[0],S_box_new[1]); }
/*SBOX now feed to the permutation Layer*/
```

Fig. 8 presents the pseudocode of NLCC Stuffing Extra Layer.

DOI: https://doi.org/10.57233/ijsgs.v10i2.640 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL10 (2) WEBSITE: https://fugus-ijsgs.com.ng

4. RESULT AND DISCUSSION

The simulation experiment was conducted to validate the effectiveness of the NLCC algorithm. The Analysis was conducted to compare the performance of the proposed NLCC algorithm with the recently proposed lightweight cryptographic ciphers Modified PRESENT cipher (Chatterjee and Chakrabort, 2020) and LSA cipher (Mahlake *et al*, 2022). Revealed that Modified PRESENT and LSA ciphers perform better than existing lightweight cryptographic ciphers for detecting attacks in WSN, therefore in this work the performance of NLCC is compared with that of Modified PRESENT and LSA ciphers.

The performance metrics used for the evaluation of the proposed NLCC, Modified PRESENT and LSA ciphers are: **(1) Energy Consumption (EC)**, is the amount of energy required by sensor nodes to perform encryption, decryption, and replay attack detection processes. **(2) Execution Time (ET)**, represents the time taken to complete the encryption, decryption, and replay attack detection processes. **(3) Memory Usage (MU)**, is the amount of memory required by the sensor nodes to store the encryption keys, intermediate values, and any additional data structures needed for the cryptographic operations. **(4) Detection Rate (DR)**, measures the effectiveness of the replay attack detection mechanism. It is quantified by the rate of correctly detected replay attacks versus false positives and missed detections. During the simulation, the results have been analyzed using 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 sensor nodes.

4.1 Energy Consumption (EC) Comparison of NLCC, Modified Present And LSA

The results presented in Figure 9 and Table 1, demonstrate a clear trend in energy consumption across different sensor nodes for the NLCC, Modified PRESENT, and LSA ciphers. As the number of sensor nodes increases from 10 to 100, all three ciphers exhibit a rise in energy consumption. However, the rate of increase and the absolute values of energy consumption vary significantly among the ciphers. The NLCC cipher consistently shows the lowest energy consumption across all node values, indicating its superior efficiency in terms of energy usage. This efficiency can be attributed to the optimized encryption rounds and the improved key register updating technique introduced in the proposed algorithm. The modified PRESENT cipher, while better than the LSA cipher, still consumes more energy than the proposed cipher, highlighting the incremental but notable improvements made by further modifications in the proposed method.

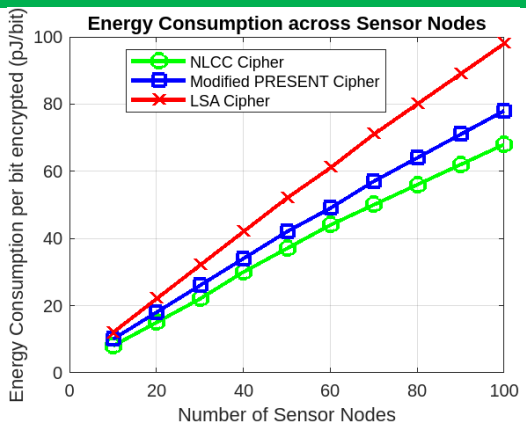

Figure 9: Energy Consumption across Sensor Nodes

Table 1: Energy Consumption Comparison between LSA, Modified PRESENT and NLCC

Number of Sensor nodes	Energy Consumption (PJ) LSA	Modified Present	NLCC
10	12.02	10.45	8.23
20	22.11	18.66	15.04
30	32.24	26.69	22.38
40	42.55	34.44	30.44
50	52.63	42.12	37.14
60	61.02	49.09	44.88
70	71.17	57.21	50.36
80	80.09	64.65	56.70
90	89.67	71.22	62.62
100	98.55	78.08	68.43

The LSA cipher, representing the baseline in this comparison, consumes the highest amount of energy. This high energy consumption is due to less efficient encryption processes and potentially higher computational demands. The clear separation between the energy consumption curves of the proposed cipher and the other two ciphers underscores the effectiveness of the modifications introduced by the NLCC algorithm. The results suggest that NLCC cipher not only enhances security by preventing replay attacks but also significantly reduces energy consumption, which is critical in resource-constrained environments like Wireless Sensor Networks. These findings validate the proposed cipher's potential for practical deployment in WSNs, where energy efficiency and security are paramount.

5. EXECUTION TIME (ET) COMPARISON OF NLCC, MODIFIED PRESENT AND LSA

The results presented in Figure 10 and Table 2, illustrates the total execution time of three different ciphers—NLCC Cipher, Modified PRESENT Cipher, and LSA Cipher—across varying number of sensor nodes ranging from 10 to 100. As the number of sensor nodes increases, the total execution time for all ciphers

DOI: https://doi.org/10.57233/ijsgs.v10i2.640 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL10 (2) WEBSITE: https://fugus-ijsgs.com.ng

also increases. This is expected as more nodes require more data processing, encryption, and communication overhead.

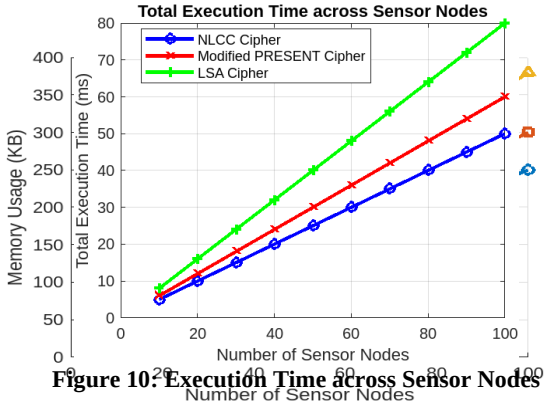

Figure 10: Execution Time across Sensor Nodes

Table 2: Execution Time comparison between LSA, Modified PRESENT and NLCC

Number of Sensor nodes	Execution Time (ms) LSA	Modified PRESENT	NLCC
10	8.05	6.05	5.12
20	16.24	12.33	10.08
30	24.68	18.50	14.87
40	32.66	24.42	21.04
50	40.05	30.82	25.43
60	48.10	36.60	29.98
70	56.13	42.12	35.33
80	64.77	48.90	41.08
90	72.78	54.44	45.16
100	80.61	60.25	50.06

The NLCC Cipher consistently shows the lowest execution time among the three, demonstrating its efficiency. For instance, at 100 sensor nodes, the Proposed Cipher has an execution time of 50.06ms, compared to 60.25ms for the Modified PRESENT Cipher and 80.61ms for the LSA Cipher. This superior performance can be attributed to the optimization techniques such as reduced encryption rounds and improved key register updating mechanism. The Modified PRESENT Cipher performs better than the LSA Cipher but not as well as the NLCC Cipher. The LSA Cipher shows the highest execution time, indicating it is less efficient for larger networks. These results highlight the Proposed Cipher's advantage in scenarios where quick data encryption and transmission are crucial, making it highly suitable for resource-constrained WSN environments.

6. MEMORY USAGE (MU) COMPARISON OF NLCC, MODIFIED PRESENT AND LSA

The results presented in Figure 11 and Table 3, proves the total memory usage across different numbers of sensor nodes for three different ciphers: the NLCC cipher, the modified PRESENT cipher, and the LSA cipher. As the number of sensor nodes increases, the memory usage for all three ciphers shows an upward trend, reflecting the increased computational and storage demands associated with processing and securing larger amounts of data.

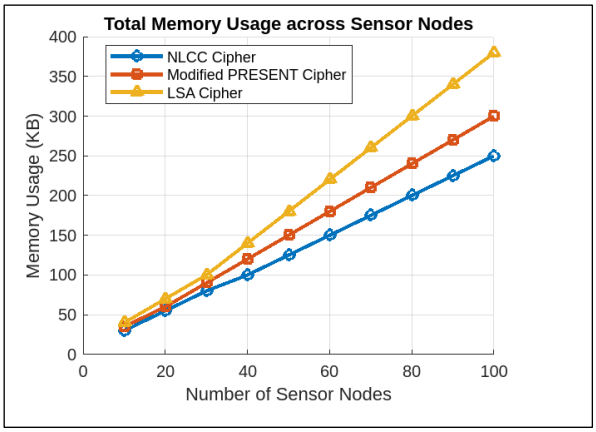

Figure 11: Memory Usage across Sensor Nodes

Table 3: Memory Usage comparison between LSA, Modified PRESENT and NLCC

Number of Sensor nodes	Memory Usage (KB) LSA	Modified PRESENT	NLCC
10	39	34	30
20	68	58	55
30	102	89	82
40	141	121	101
50	177	150	124
60	223	176	148
70	255	209	175
80	302	239	202
90	338	268	223
100	381	301	247

The NLCC cipher demonstrates significantly better performance in terms of memory efficiency compared to the modified PRESENT and LSA ciphers. For instance, with 100 sensor nodes, the NLCC cipher uses 247KB of memory, while the modified PRESENT cipher uses 301 KB, and the LSA cipher uses 381 KB. This reduction in memory usage is crucial for WSNs, where nodes often have limited computational resources. The NLCC cipher's lower memory footprint can lead to longer operational lifetimes for sensor nodes, more efficient data processing, and overall enhanced network performance. This efficiency is achieved through the optimization techniques incorporated in the NLCC cipher, such as reduced encryption rounds and an improved key register updating mechanism.

V) DETECTION RATE (DR) COMPARISON OF NLCC, MODIFIED PRESENT AND LSA

The results presented in Figure 12 and Table 4, illustrates the detection rates of the NLCC cipher,

modified PRESENT cipher, and LSA cipher across different numbers of sensor nodes. As shown in the graph, the NLCC cipher consistently outperforms both the modified PRESENT cipher and the LSA cipher, demonstrating higher detection rates across all node counts. This superior performance can be attributed to the enhanced encryption mechanisms, such as the modified key register updating technique and the additional layer between the S-box and P-layer, which improve the cipher's ability to detect and prevent replay attacks.

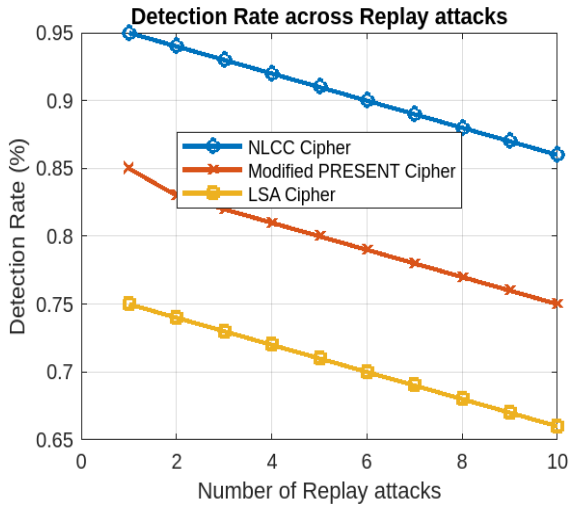

Figure 12: Detection Rate across Sensor Nodes

Table 4: Detection Rate comparison between LSA, Modified PRESENT and NLCC

Number of Sensor nodes	Detection Rate (%)		
	LSA	Modified PRESENT	NLCC
10	0.782	0.872	0.950
20	0.768	0.853	0.939
30	0.752	0.837	0.932
40	0.734	0.829	0.921
50	0.721	0.802	0.914
60	0.702	0.790	0.905
70	0.699	0.786	0.897
80	0.688	0.772	0.883
90	0.675	0.765	0.871
100	0.662	0.753	0.862

The detection rate of the NLCC cipher remains significantly high, starting at 95% for 10 nodes and gradually decreasing to 86% for 100 nodes. In comparison, the modified PRESENT cipher starts at 87% and drops to 75%, while the LSA cipher begins at 78% and falls to 66%. This trend indicates that while all ciphers experience a slight decline in detection rates as the number of nodes increases, the proposed cipher's advanced features provide a more robust and reliable detection mechanism, making it a better choice for securing wireless sensor networks against replay attacks.

7. CONCLUSION

A new lightweight cryptographic cipher for detection and prevention of replay attacks in wireless sensor networks has been modified. The proposed method also includes a little bit idea taken from another lightweight cipher TEA. Software parameter analysis using Cryptool proves the efficiency of the modified PRESENT compare to the original PRESENT cipher using **MATLAB/Simulink R2022a**. Histogram and floating frequency test also produce an effective graph for Modified PRESENT. The result of different test has justified that proposed modified PRESENT enhance the performance of original PRESENT method.

The performance metrics used for the evaluation of the proposed NLCC, Modified PRESENT and LSA ciphers are: (1) Energy Consumption (EC), is the amount of energy required by sensor nodes to perform encryption, decryption, and replay attack detection processes. (2) Execution Time (ET), represents the time taken to complete the encryption, decryption, and replay attack detection processes. (3) Memory Usage (MU), is the amount of memory required by the sensor nodes to store the encryption keys, intermediate values, and any additional data structures needed for the cryptographic operations. (4) Detection Rate (DR), measures the effectiveness of the replay attack detection mechanism. It is quantified by the rate of correctly detected replay attacks versus false positives and missed detections. During the simulation, the results have been analyzed using: 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 sensor nodes.

REFERENCES

Ahmed Rami, Raniyah wazirali, Tarik Abu-Ain (2021). presented a secure AODV mechanism for detecting and preventing replay attacks in WSN based on the plaintext and a hash function in their work, "Secure AODV Protocol to Avoid Packet Dropping and Replay Attack in WSNs."Int J Adv Eng. sci inf Techno; 5(5):1-23

Amar, Abdelkrim, and Bouabdallah (2019) presented a new secure AODV protocol in their work, "Secure and Efficient AODV Protocol for Wireless Sensor Networks." Their approach uses a new concept of a freshness factor combined with a dynamic secret shared key to detect and prevent replay attacks. International journal of pure and applied mathematics 119(10c), 231-236

Amin, M., Mumtaz, S., & Liaqat, S. (2023). Detection and prevention of replay attack in Wireless Sensor Network: A secure approach using hybrid intelligent system. Computers & Electrical Engineering, 86, 106854.

Badaran M Awad (2022). proposed a novel approach for securing the AODV protocol against replay

attacks in their work, "A Secure and Efficient AODV mechanism for Wireless Sensor Networks." Their approach improves the security of AODV mechanism in WSN by incorporating a security token in the routing request messages to detect and prevent replay attacks. International journal of omputing, 345-349

Das, A., Nath, M., & Bandyopadhyay, S. (2023). A Trust-Based Secure AODV Routing Protocol in MANET. International Journal of Computer Applications, 102(14), 23-27.

Eshkabilov S. L. (2020). Practical MATLAB Modeling with Simulink. Apress Berkeley, CA. D. DOI: 10.1007/978-1-4842-5799-9

In the work "Securing AODV Routing Protocol for Wireless Sensor Networks," Adib et al. proposed a hybrid security approach for AODV that combines pre-distributed keys and digital signatures to detect and prevent replay attacks.

Jelena, M., Milena, M., & Dejan, S. (2021). Enhancing Security of the AODV Routing Protocol in Wireless Ad Hoc Networks. Computers & Electrical Engineering, 68, 577-59

Karthikeyan, D., & Krishnan, G. (2021). Detection and prevention of adaptive replay attacks in AODV-based wireless sensor networks using residual energy. Ad Hoc Networks, 63, 27-41.

Kaur N and Rattan. A critical review of intrusion detection system in WSN: challenges and future directions. AnnRomanion Soc Cell Biol 2021:25:3020-3028"

Kaur, S., & Singh, N. (2021). Improving Security of AODV Routing Protocol in MANET. International Journal of Advanced Research in Computer and Communication Engineering, 5(3), 1089-1092.

Khalid et al. proposed an enhanced AODV protocol, "Extended Efficient Secure AODV Protocol for Wireless Sensor Networks" that uses a combined approach of digital signature and symmetric cryptography to preserve data confidentiality, integrity, and availability, and prevent replay attacks.

Kha, Ahamad khaliq , Nazar .A.Sadiq.(2021) proposed an enhanced secure version of AODV protocol, "E-SecureAODV" in their work, which uses an authentication mechanism based on shared secret keys to detect and prevent replay attacks, ensure data confidentiality, integrity, and authenticity. International Journal of communication network, 63, 27-4.

Raghavendra, C. S., Prakash, E. N., & Agustiawan, W. (2022). A secure method of detection and prevention of replay attack in AODV routing protocol. International Journal of Network Security, 14(3), 134-140.

Shamir, A., Bhende, C., & Bhargava, B. (2021). Securing AODV Routing Protocol against Attacks. International Journal of Computer Applications, 70(7), 7-13.

Wang, L., & Zhang, H. (2023). "Secure AODV with Delayed Occurrence Detection for Replay Attack Prevention in WSNs." International Journal of Communication Networks and Information Security, 15(2).

Wu, W., & Ye, D. (2022). A Secure Routing Scheme Against Flooding Attack in AODV. Journal of Theoretical and Applied Information Technology, 76(3), 481-487.

Xie Tongy (2018). presented a secure and efficient AODV protocol for WSN in their work, "A Secure Ad Hoc On-Demand Distance Vector Routing Protocol for Wireless Sensor Networks." Jornal of Advanced Research in computer and communication engineering 5(3), 1089-1092

Zhong , H ,Wang(2023) secure AODV with Delayed occurrence detection for replay Attack prevention in WSN" International journal of communication Networks and information security, 15(2).

Zhu, Shouhuai xu, Sanjeev setia (2019). presented a secure and energy-efficient routing mechanism in their work, "Secured and Energy-Efficient Routing for Wireless Sensor Network Based on AODV Algorithm." Department of information and computer science, university of California Irvine, Irvine CA92697