JOURNAL OF TECHNIQUES

Journal homepage: http://journal.mtu.edu.iq

RESEARCH ARTICLE - ENGINEERING

Applying TTIED-CMYK Algorithm in Wireless Sensor Networks Based on Raspberry pi and DHT-11

Noor Sattar Noor[1*], Dalal Abdulmohsin Hammood[1], Ali Al-Naji[2]

[1] Engineering Technical College-Baghdad, Middle Technical University, Baghdad, Iraq.

[2] School of Engineering, University of South Australia, Adelaide, Australia.

[*] Corresponding author E-mail: bc0055@mtu.edu.iq

Article Info.

Article history:

Received
15 June 2022

Accepted
06 August 2022

Publishing
30 September 2022

Abstract

Recently, there has been a wide and continuous development in wireless sensor networks WSNs. These networks are directly employed in our daily lives, so it has become necessary to maintain the confidentiality of information in these networks. This paper provided a detailed explanation of the types of attackers according to their layer, in addition to the design of a wireless sensor network consisting of a temperature and humidity sensor called the DHT-11 and a Raspberry Pi to implement the Text-To-Image Encryption/Decryption algorithm based on CMYK mode (TTIED-CMYK) in these networks. An encrypted image with dimensions of 2×2 and a size not exceeding 70 bytes was obtained for a text consisting of eleven characters. In addition to that, the encryption time is very short, not exceeding 1 microsecond.

Publisher : Middle Technical University

Keywords: Text-to-Image Encryption (TTIE); TTIED-CMYK algorithm; Wireless Sensor Networks (WSNs); Raspberry Pi; DHT-11.

1. Introduction

Nodes are devices whose purpose is to measure natural phenomena such as temperature, pressure, and humidity or to measure abnormal phenomena such as the movement of enemies, current, voltage, etc [1, 2]. The wireless sensor network requires many conditions. Firstly, an environment or a field for event sensing, for example, an enemy area. Secondly, the number of sensors is very large. Thirdly, a base station to receive information from sensors and send it to the control center. Finally, a monitoring and control center to take the appropriate action [3].

In addition to that, the nodes can sense and perform the necessary calculations and send them to the main station and then to the monitoring unit. Wireless sensor networks have several characteristics and are small in size. Therefore, restrictions are imposed on them, which are limited to power, communication, sensors, calculations, and operating systems for these sensors. Sensors are usually grown in environments with harsh conditions. Most of the developers tried to design nodes that have high capacity and low cost and send data between the nodes and the base station quickly and securely [4-6].

There must be procedures in place to prevent any attack on such networks. The broadcast mechanism is used to deliver and receive data across nodes [7]. As a result, there are various vulnerabilities via which attackers can get access to and alter network resources. On the one hand, there must be a hidden and secure means to know the nodes connecting them, and the information exchanged between them must be encrypted with difficult-to-break techniques on the other. The TTIED-CMYK algorithm is introduced in this study for use on data sent between nodes [8]. This technique has several advantages, the most notable of which is that it is lightweight, takes little time to conduct encryption, and does not require a large bandwidth. In other words, this approach conforms to the constraints placed on wireless sensor network nodes.

In the rest of this paper, WSNs attacks are described in section 2, WSNs security requirements are explained in section 3, and the suggested solution is described in section 4. The results are provided in section 5. The last section is the conclusion.

Nomenclature			
TTIE	Text-To-Image Encryption Algorithm	PUF	Physical Unclonable Function
TTIED-CMYK	Text-To-Image Encryption Decryption CMYK mode	DHT-11	Digital Temperature and Humidity
WSNs	Wireless Sensor Networks	DoS	Denial of Service

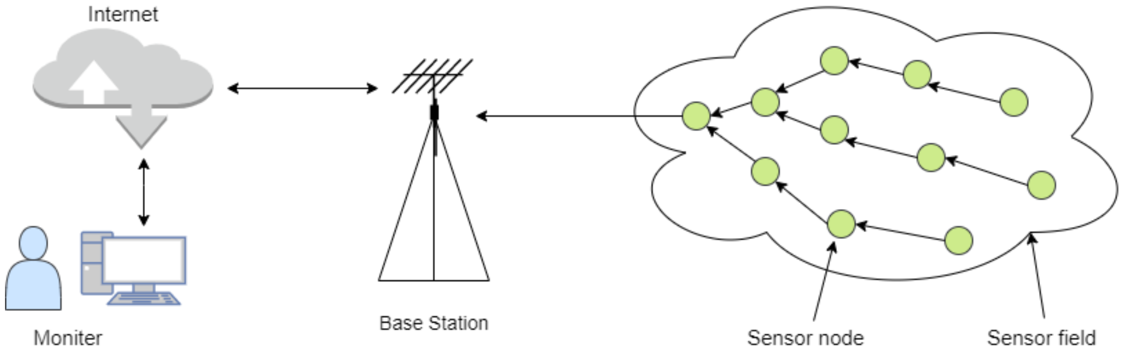


Fig 1. The structure of WSNs

2. Attack in WSNs

In this section, we explain the different types of attacks that lead to network damage and threaten its confidentiality. In this paper, the attackers are classified according to the layer that they can be attacked, as follows.

2.1. Attacks on the Physical Layer

The attack in this layer is considered one of the most challenging types of attack. There are many types of attackers on this layer, as follows:

2.1.1. Attack on the Side Channel

This attack can also obtain information that could compromise the system by using information (for example, the computation time for performance of encryption algorithms, power consumption during the computation process, electromagnetic waves emitted by devices, etc.) from sensors. The possibility of this attack by obtaining some important information about the sensor's operating system, such as encryption algorithms, transmission paths, calculations, and the sensitivity mechanism. This type of attack can be avoided with Physical Unclonable Function (PUF) [9, 10].

2.1.2. Camouflage

Camouflaging is a type of attack that occurs when nodes in WSN are breached. In other words, additional nodes are entered as the original node by the attacker, which is called malicious nodes [11, 12] whose purpose is to camouflage and forward false information.

2.1.3. Node Replication

There is a type of attacker who tries to replicate the physical access to the information inside the nodes. When it succeeds in accessing the nodes' information, it creates a node similar to the original nodes[13]. This attack causes confusion, loss of information and service, and jamming. In other words, the repeated nodes lead to network weakness and the integrity of the confidentiality of its information [14].

2.1.4. Node Capture

In this type, the attacker tries to add forged nodes to the original nodes. These nodes can communicate and adapt to the network completely so that they can eavesdrop on the network information [15, 16].

2.1.5. Jamming

It is the most dangerous type of wireless sensor network, as it jams the network and cuts off communication between the nodes due to interference in frequencies [17].

2.1.6. Tampering

The attacker tries to gain access to the physicist in the network. If he succeeds, he analyzes the original nodes and extracts their information, such as encryption algorithms, data transmission mechanisms, and other information. This type of attack can be prevented by using isolation between nodes [18].

2.2. Attacks on the Data Link Layer

The main function of this layer is to share channels between nodes. There are many attackers on it, as follows:

2.2.1. Traffic Analysis

This type of attack is used to discover the mechanism of communication between the nodes. This is done by studying the traffic of data within the network [19]. This type is dedicated to the master nodes called the sink, which has the main network information such as the number of nodes, communication mechanism, encryption and decryption algorithms, and other information [20].

2.2.2. Collision

This type occurs when some of the planted nodes within the network are damaged, which leads to disconnection and loss of paths between nodes. In addition, it leads to poor sensitivity to the events to be known by the observers [21].

2.2.3. Exhaustion

This attack focuses on energy depletion by repeating transmissions and increasing path loops [22].

2.2.4. Unfairness

In this type, the attacker tries to access the nodes to use them in an abusive manner, which leads to late receipt of data and loss of time in the network [23].

2.3. Attacks on the Network Layer

A network layer attack is frequently a denial of service (DoS) attack intended to bring the network to a standstill. Furthermore, spoofing, rotation, and replay attacks jeopardize the integrity of the data. The network is designed on a custom architecture with WSN characteristics, which is the cause of these various attacks [24]. Derives from the network's ad-hoc structure, which includes WSN features.

2.3.1. Eavesdropping

Collecting data between sensors by the attacker is called eavesdropping, which leads to the possibility of killing the network through frequency interference and information loss in wireless sensor networks [25].

2.3.2. Stealthy Packet Dropping

This type of attack occurs in WSNs easily because it depends on multiple hops when transmitting between nodes. The principle of operation of this attack depends on the addition of forged nodes that misleads the original nodes and disrupts the transmission of data between destinations [26].

2.3.3. Spoofed and replayed routing information

This type of attack is intended to increase the time allotted to receive data between nodes, restrict traffic, and increase path loops [27].

2.4. Attacks on the Transport Layer

As mentioned earlier, wireless sensor networks suffer from several resources, so the attacker in this layer tries to exploit the transmission and reception because it has specific characteristics.

2.4.1. Flooding

This type wastes network resources by ignoring connection requests or sending unnecessary data to flood the network and waste its energy [28].

2.4.2. Desynchronization

This type attempts to prevent asynchrony between nodes by sending corrupt data and a dummy identifier [29].

2.5. Attacks on the Application Layer

This type of attack is divided into two categories. The first is overwhelming, which is dedicated to wasting energy in the network by increasing the sensitivity of the sensor and sending sensitive data between nodes [30]. The second is called the Deluge. This type is similar to viruses. The programming system aims and works to damage the system to avoid this type of attack using programming with strong authenticators [31].

3. WSNs Security Requirements

As mentioned previously, WSNs have several advantages and also suffer from limitations, so it is dealt with accurately. The twelve security requirements for WSN networks [7] are presented in this section and may be seen in Fig. 2.

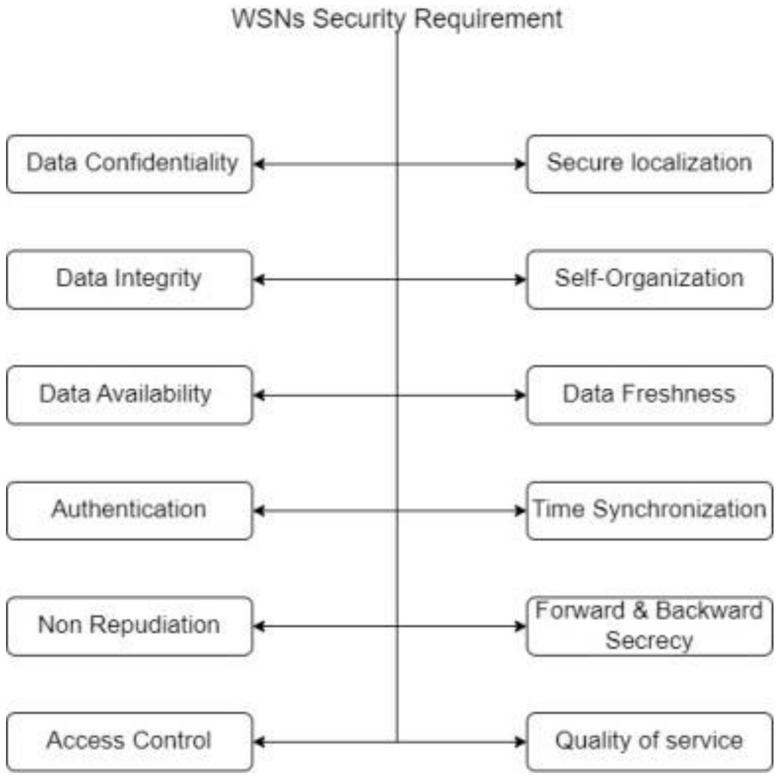


Fig 2. WSN security requirements

4. The Proposed Solution

In this section, a wireless sensor network WSN is designed to conduct the tests required to use the TTIED-CMYK algorithm, which is intended to maintain the confidentiality of data exchanged between sensor nodes.

The proposed network consists of a temperature and humidity sensor called DHT-11, as shown in Fig. 3, connected to a Raspberry Pi version 3, where the required calculations are performed inside the raspberry. In other words, the Raspberry Pi contains the TTIED-CMYK algorithm, which in turn converts the sensitive data via DHT-11 into a color image. This image represents the ciphertext that is sent to the receiving station, as shown in Fig.4. There is a type of attacker trying to access the exchanged data between sensor nodes. Therefore, this algorithm was used because it has a high encryption strength, and it takes a lot of time to try to break it [8].

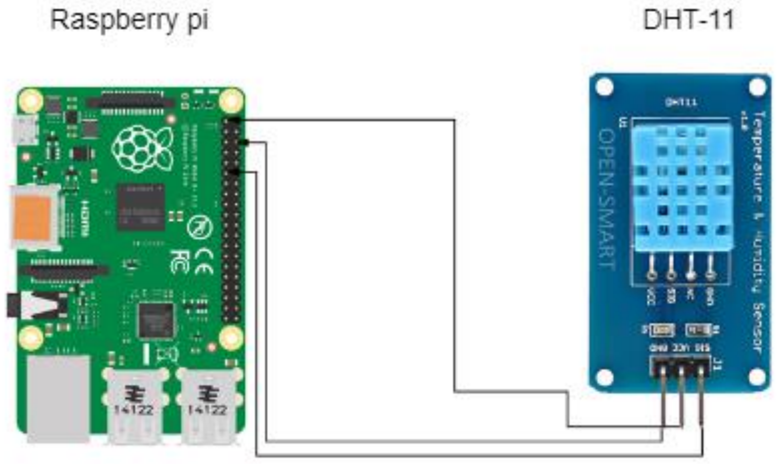


Fig 3. The proposed sensor (temperature and humidity sensor)

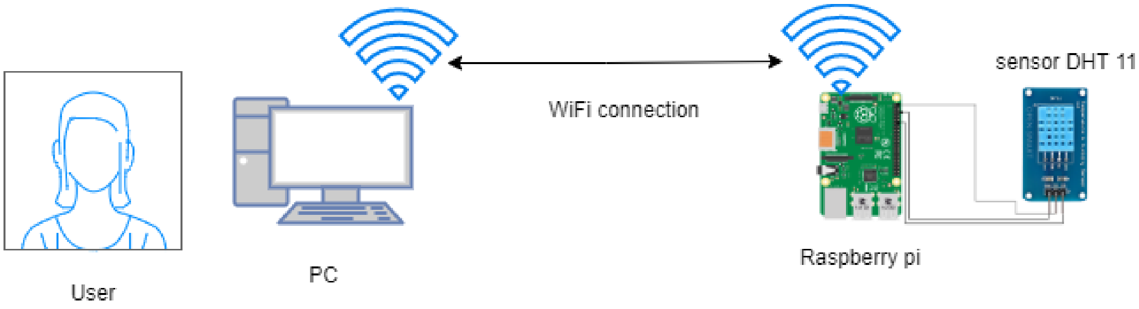


Fig 4. The proposed design of WSNs

5. Results

5.1. Device specification

All experiments were carried out using Python on raspberry pi v+3 and a computer with an Intel Core i7, 2.6GHz CPU, 8 GB of RAM, and a 64-bit Windows 10 operating system.

5.2. Apply TTIED-CMYK in WSNs

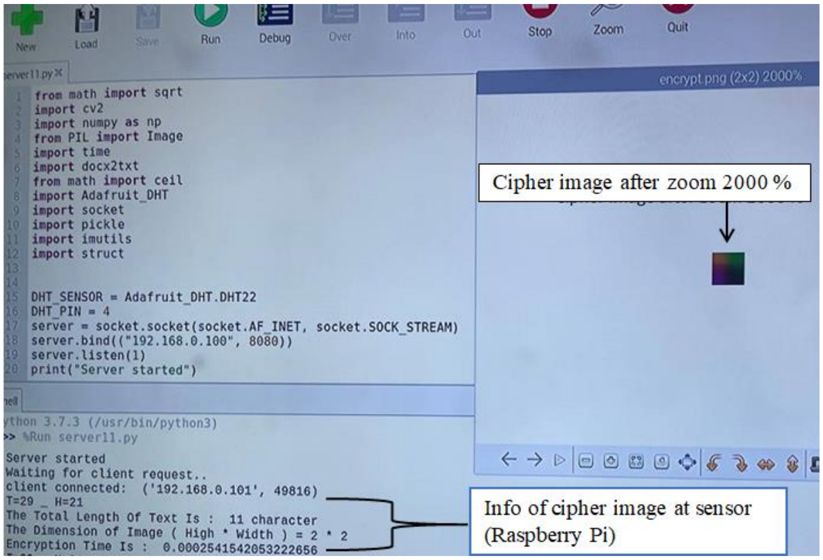
DHT-11 senses the data and displays it as a text with eleven characters "T=29 _ H=21", which it then transmits to the raspberry (the sender) as shown in Fig.5, which has the proposed algorithm TTIED-CMYK, which converts the text into a 2×2 image with a size of 70 bytes. This image is sent to the control and monitoring unit (the receiver), as shown in Fig. 6, which works to decrypt the encrypted image to obtain the original text. The executed time is very short, not exceeding 1 microsecond.

5.3. Comparison of TTIED-CMYK with other encryption algorithms

Table 1 shows the comparison of the proposed algorithm with some other algorithms in terms of key length, language support, encryption time, and ciphertext storage space.

Table 1 The comparison of TTIED-CMYK with other encryption algorithms.

Algorithm	Key length (in bytes)	Language support	Encryption time (second)	Storage (byte)
RC5	256	English only	2.09 ms	268
RC6	256		Cannot run in WSNs	Cannot run in WSNs
AES Rijndael	256			
WSN-CSB[32]	128		8.01ms	274
TTIED-CMYK	1024	English and Arabic	1 µs	70



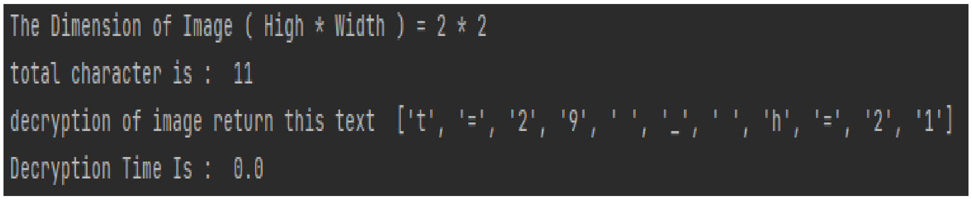
```
from math import sqrt
import cv2
import numpy as np
from PIL import Image
import time
import docx2txt
from math import ceil
import Adafruit_DHT
import socket
import pickle
import imutils
import struct


DHT_SENSOR = Adafruit_DHT.DHT22
DHT_PIN = 4
server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind(("192.168.0.100", 8080))
server.listen(1)
print("Server started")
```

```
ython 3.7.3 (/usr/bin/python3)
>> %Run server11.py

Server started
Waiting for client request..
client connected:  ('192.168.0.101', 49816)
T=29 _ H=21
The Total Length Of Text Is :  11 character
The Dimension of Image ( High * Width ) = 2 * 2
Encryption Time Is :  0.0002541542053222656
```

Fig 5. The image is encrypted by the user (raspberry pi)



```
The Dimension of Image ( High * Width ) = 2 * 2

total character is :  11

decryption of image return this text  ['t', '=', '2', '9', ' ', '_', ' ', 'h', '=', '2', '1']

Decryption Time Is :  0.0
```

Fig 6. The image received after being decrypted at the receiver (PC)

6. Conclusion

In this paper, the TTIED-CMYK algorithm was implemented in wireless sensing networks to prevent the attacker's access to the data exchanged between nodes to the control and monitoring center. An encrypted image with dimensions of 2×2 and a size not exceeding 70 bytes was obtained for a text consisting of eleven characters. Moreover, the encryption time is very short, not exceeding 1 microsecond. As a result, the application of this algorithm to protect information is commensurate with the resource constraints imposed on wireless sensor networks. In future work, the TTIED-CMYK algorithm will be applied to IoT.

Acknowledgment

We extend our thanks and appreciation to the official sponsor of the conference, Middle Technical University, Electrical Engineering Technical College-Baghdad, Iraq, for the support and encouragement for the dissemination of scientific engineering research.

References

[1] A. Albakri, L. Harn, and S. Song, “Hierarchical Key Management Scheme with Probabilistic Security in a Wireless Sensor Network (WSN),” Secur. Commun. Networks, vol. 2019, 2019, doi: 10.1155/2019/3950129.

[2] M. Hema Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, “Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN,” J. Ambient Intell. Humaniz. Comput., vol. 12, no. 5, pp. 5287–5295, 2021, doi: 10.1007/s12652-020-02007-w.

[3] D. G. Padmavathi and M. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” vol. 4, no. 1, pp. 1–9, 2009, [Online]. Available: http://arxiv.org/abs/0909.0576.

[4] M. Dener, “Security analysis in wireless sensor networks,” Int. J. Distrib. Sens. Networks, vol. 2014, 2014, doi: 10.1155/2014/303501.

[5] A. Karakaya and S. Akleylek, “A survey on security threats and authentication approaches in wireless sensor networks,” 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018-January, pp. 1–4, 2018, doi: 10.1109/ISDFS.2018.8355381.

[6] A. Rani and S. Kumar, “A survey of security in wireless sensor networks,” 3rd IEEE Int. Conf. , pp. 3–7, 2017, doi: 10.1109/CIACT.2017.7977334.

[7] D. S. Ibrahim, A. F. Mahdi, and Q. M. Yas, “Challenges and Issues for Wireless Sensor Networks : A Survey,” J. Glob. Sci. Res., vol. 6, no. 1, pp. 1079–1097, 2021, [Online]. Available: https://www.researchgate.net/publication/349738262.

[8] N. S. Noor, D. . Hammood, A. Al-Naji, and J. Chahl, “A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication,” Computers, vol. 11, no. 39, 2022, [Online]. Available: https://doi.org/10.3390/computers11030039.

[9] Y. Cao, X. Zhao, W. Ye, Q. Han, and X. Pan, “A compact and low power RO PUF with high resilience to the EM side-channel attack and the SVM modelling attack of wireless sensor networks,” Sensors (Switzerland), vol. 18, no. 2, 2018, doi: 10.3390/s18020322.

[10] T. Schneider, A. Moradi, and T. Güneysu, ParTI - Towards combined hardware countermeasures against side-channel and fault-injection attacks, vol. 9815. 2016.

[11] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks, and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," Proc. IEEE Int. Conf. Signal Process. Commun. ICSPC 2017, vol. 2018-January, no. July, pp. 288–293, 2018, doi: 10.1109/CSPC.2017.8305855.

[12] R. den Hollander et al., “Adversarial patch camouflage against aerial detection,” no. September 2020, p. 11, 2020, doi: 10.1117/12.2575907.

[13] L. Li et al., “A Secure Random Key Distribution Scheme Against Node Replication Attacks in Industrial Wireless Sensor Systems,” vol. XX, no. X, pp. 1–10.

[14] L. Sujihelen, C. Jayakumar, and C. Senthilsingh, “SEC approach for detecting node replication attacks in static wireless sensor networks,” J. Electr. Eng. Technol., vol. 13, no. 6, pp. 2447–2455, 2018, doi: 10.5370/JEET.2018.13.6.2447.

[15] R. Bhatt, P. Maheshwary, P. Shukla, P. Shukla, M. Shrivastava, and S. Changlani, “Jo urn,” Comput. Commun., 2019, doi: 10.1016/j.comcom.2019.09.007.

[16] R. Gooding-townsend, S. T. E. N. Holder, and B. Ingalls, “Displacement of Bacterial Plasmids by Engineered Unilateral Incompatibility,” IEEE Life Sci. Lett., vol. 1, no. August, pp. 19–21, 2015, doi: 10.1109/LLS.2015.2465839.

[17] O. Almomani, "An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks," mdpi , Sensors, vol. 20, no. 2311, pp. 1–19, 2020, doi: 10.3390/s20082311.

[18] D. Huang, W. Liu, and J. Bi, “Data tampering attacks diagnosis in dynamic wireless sensor networks,” Comput. Commun., vol. 172, no. March, pp. 84–92, 2021, doi: 10.1016/j.comcom.2021.03.007.

[19] N. Alqudah and Q. Yaseen, “ScienceDirect ScienceDirect Machine Learning for Traffic Analysis : A Review Machine Learning for Traffic Analysis : A Review,” Procedia Comput. Sci., vol. 170, pp. 911–916, 2020, doi: 10.1016/j.procs.2020.03.111.

[20] J. R. Ward, M. Younis, and J. R. Ward, “Cross-layer traffic analysis countermeasures against adaptive attackers of wireless sensor networks,” Wirel. Networks, vol. 9, 2019, doi: 10.1007/s11276-019-02003-9.

[21] A. Kumari, N. Shrivastava, and N. K. Raman, “A Prime Exploration of Collision Detection in WSN :,” vol. 4, no. 4, pp. 241–244, 2019, doi: 10.1038/ncomms852.

[22] J. Kaushik and D. Academics, “Security Technique against Power Exhausting Attacks in WSN,” vol. 25, no. 6, pp. 4640–4667, 2021.
[23] I. Journal, “A Critical Analysis on Network Layer Attacks in Wireless Sensor Network,” Int. Res. J. Eng. Technol., vol. 5, no. 2, pp. 2395–0072, 2018.
[24] L. Alsulaiman, S. Al-ahmadi, and S. Arabia, "PERFORMANCE E VALUATION OF M ACHINE L EARNING TECHNIQUES FOR DOS DETECTION IN," vol. 13, no. 2, pp. 21–29, 2021, doi: 10.5121/ijnsa.2021.13202.
[25] H. H. Syed, “WSNs Prone to Swap Attacking and Eavesdropping,” no. July 2019, 2022.
[26] R. Varatharajan and A. P. Preethi, “Stealthy attack detection in multi-channel multi-radio wireless networks,” Springer Multimed Tools Appl 2backgr., vol. 7, no. 9, pp. 2001–2018, 2018.
[27] K. S. Adu-Manu, N. Adam, C. Tapparello, H. Ayatollahi, and W. Heinzelman, “Energy-harvesting wireless sensor networks (EH-WSNs): A review,” ACM Trans. Sens. Networks, vol. 14, no. 2, 2018, doi: 10.1145/3183338.
[28] L. Hn, S. Anand, and S. Sinha, “Flooding Attack in Wireless Sensor Network-Analysis and Prevention,” Int. J. Eng. Adv. Technol., vol. 8, no. 5, 2020.
[29] J. S. Alshudukhi and Z. G. Al-mekhlafi, “Desynchronization Traveling Wave Pulse-Coupled-Oscillator Algorithm Using a Self-Organizing Scheme for Energy-Efficient Wireless Sensor Networks,” 2020, doi: 10.1109/ACCESS.2020.3034577.
[30] M. Nafis, U. Islam, A. Fahmin, and S. Hossain, “Denial ‐ of ‐ Service Attacks on Wireless Sensor Network and Defense Techniques,” Wirel. Pers. Commun., no. 0123456789, 2020, doi: 10.1007/s11277-020-07776-3.
[31] A. Kardi and R. Zagrouba, “Attacks classification and security mechanisms in Wireless Sensor Networks,” Adv. Sci. Technol. Eng. Syst. J., vol. 4, no. 2415–6698, pp. 229–243, 2019, doi: 10.25046/aj040630.
[32] Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. “A novel block encryption algorithm based on chaotic S-box for wireless sensor network”. *IEEE Access*, vol.*9*, pp. 53079-53090, 2019.