Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 9
September 2023

Intrusion Detection and Preventing Resource Exhaustion in Wireless Sensor Networks

Hariprasad N
Department of Computer Science
School of Computing, Mysore
Amrita Vishwa Vidyapeetham
India

Santhosh Kumar B J
Department of Computer Science
School of Computing, Mysore
Amrita Vishwa Vidyapeetham
India

Abstract- Wireless Sensor Networks (WSNs) are used in various applications such as environmental monitoring, surveillance, and healthcare. However, the limited processing power and battery life of WSN nodes make them vulnerable to resource exhaustion attacks. Resource exhaustion attacks can cause a node to become unusable, which can affect the entire network. In this paper, we focus on two types of resource exhaustion attacks: Slowloris and ping of death. Slowloris attacks involve an attacker sending small packets of data to a node at a slow rate, while ping of death attacks involves an oversized packet that can consume a large amount of a node's processing power and memory. To prevent these attacks, we propose various intrusion detection and prevention techniques, including access control mechanisms, packet filtering, and traffic shaping. We also emphasize the importance of regularly updating ping software and firmware to patch any vulnerabilities that may be exploited by attackers. By implementing these techniques, WSNs can be better protected against resource exhaustion attacks, enhancing the overall security and reliability of the network. The security of WSNs can be improved by putting intrusion detection systems (IDS) in place. IDS can track network activity and spot patterns or oddities that could be signs of resource exhaustion attacks. Once the attack has been identified, proper countermeasures can be implemented, such as blocking malicious traffic or isolating the impacted node.

Keywords - Ping of death, Slowloris ,Resource exhaustion , Packet traffic.

I. Introduction

Wireless Sensor Networks (WSNs) have emerged as a popular technology in recent years due to their ability to collect data in real-time from various applications such as environmental monitoring, surveillance, and healthcare. However, WSNs are vulnerable to attacks due to their limited processing power and battery life. Resource exhaustion attacks are a common type of attack that can affect the performance of WSN nodes, causing them to become unusable and disrupting the overall functionality of the network. Slowloris and ping of death are two common types of resource exhaustion attacks that can be used to target WSNs. Slowloris attacks involve an attacker sending small packets of data to a node at a slow rate, while ping of death attacks involves an oversized packet that can consume a large amount of a node's processing power and memory. In this paper, we focus on the detection and prevention of Slowloris and ping of death attacks in WSNs. We propose various intrusion detection and prevention techniques, including access control mechanisms, packet filtering, and traffic shaping. These techniques can help detect and prevent resource exhaustion attacks, improving the overall security and reliability of the WSN. We also highlight the importance of regularly updating software and firmware to patch any vulnerabilities that may be exploited by attackers.

II. Literature Survey

The Cumulative Sum (CUSUM) technique is used in the research paper by Kumar and Gowda to

provide a unique method for locating and countering UDP Reflection Amplification Attacks in wireless sensor networks (WSNs). The study recognises the value of strong security mechanisms in WSNs to thwart this specific type of assault. It explores the subtleties of the suggested method and clarifies how it might be used in practise for detection and mitigation[1]. The approach described in this paper can be used to stop TCP SYN flooding assaults in Wireless Sensor Networks (WSNs). According to the underlying protocol, the authors' proposed Protocol Dependent Detection and Classification System (PDDCS) analyses network traffic and categorises SYN packets. By precisely identifying and counteracting TCP SYN flooding assaults, the study intends to improve the security of WSNs while also boosting the network's overall performance and resilience [2]. The analysis and mitigation of flooding threats in wireless sensor networks (WSNs) are covered in the study. It offers insights into various flooding attack types, suggests defences against them, and seeks to raise WSN security and dependability. In order to protect network infrastructure and ensure successful data communication, the study addresses resource depletion and interruption brought on by excessive data traffic [3]. The paper discusses SQL injection, a flaw in web applications' security. It proposes a way to analyse code, find weaknesses, and put up barriers in order to detect and prevent SQL injection attacks. The goal of the study is to strengthen online application security, safeguard sensitive data, and uphold the confidentiality and integrity of information [4]. The analysis and prevention of flooding attacks in wireless sensor networks are covered in the paper named "Flooding attack in wireless sensor network-analysis and prevention". The authors examine different flooding attack types and provide defences to strengthen the security and dependability of WSNs. In order to ensure good data transfer in WSNs, the study intends to offer insights and practical remedies for reducing flooding threats [5].The paper focuses on how to use IDS to increase the security of WSNs. The study gives a thorough analysis of several intrusion detection strategies and techniques that are designed expressly for WSNs. It examines the complexities and challenges associated with intrusion detection in WSNs and offers insightful information on the creation and application of effective IDS solutions[6]. The impact and effectiveness of resource exhaustion attacks against wireless mobile devices are thoroughly examined in this study. It assesses various resource exhaustion approaches and analyses the effects they have on the functionality and performance of these devices. This research, which was published in the journal Electronics, provides in-depth insights into the vulnerabilities associated with resource exhaustion assaults and suggests potential defences against them in the context of mobile devices.[7]. The implementation of data mining techniques is explicitly examined in order to enhance intrusion detection and classification within WSNs. The study offers a thorough analysis of several intrusion detection approaches and suggests a data mining-based strategy for effective and efficient intrusion detection[8]. The research paper focuses on the creation of an intrusion detection system (IDS) suited for the detection and mitigation of Ping of Death attacks in Internet of Things (IoT) networks. The study discusses the security issues that these attacks in IoT contexts provide. It offers a thorough investigation of the suggested IDS, covering its conception, installation, and assessment of its performance in identifying and averting Ping of Death attacks[9]. The study provides comprehensive insights into the use of mathematical and cryptographic techniques for successfully reducing DDoS assaults in WSNs. It provides a thorough examination of the guiding ideas and techniques used to defend against such assaults, putting particular emphasis on their mathematical and cryptographic elements[10].

III. Methodology

a. Building Network Model

Building a network model for a WSN involves several steps, including defining the network topology, selecting the sensor nodes and their attributes, and configuring the communication protocols. The first step is to define the network topology. This involves selecting the type of topology that best suits the application requirements.

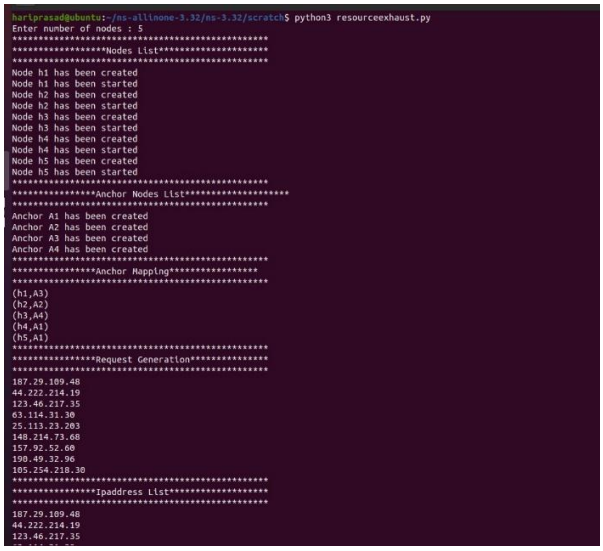

Figure1: node creation and anchor node creation and ip address list.

b. Generating Packet Traffic

Generating packet traffic is an essential aspect of testing the performance of a Wireless Sensor Network (WSN). Packet traffic can be generated using various methods, including random packet generation and scripted packet generation. Random packet generation involves generating packets at random intervals and with random content.

To generate packet traffic, the NS3 simulator can be used, which provides several options for packet generation. The application layer protocol can be selected to define the format and content of the packets.

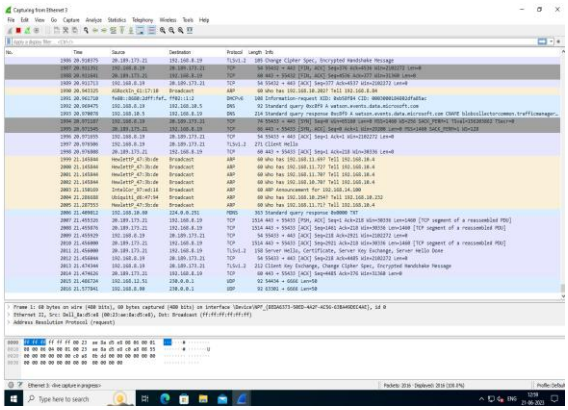

Figure2: Generating packet Traffic

The packet generation can be configured to simulate different traffic patterns, such as bursty traffic, periodic traffic, or constant bit rate traffic. Packet traffic can be analyzed using tools such as Wireshark to measure performance metrics such as packet delivery ratio, delay, and throughput. Overall, generating packet traffic is an important aspect of testing the performance and effectiveness of a WSN, and the appropriate method of packet generation should be selected based on the desired scenario and testing requirements.

c. Injecting intrusion attacks

Injecting intrusion attacks into a Wireless Sensor Network (WSN) is crucial in testing the effectiveness of intrusion detection and prevention mechanisms. Two common types of intrusion attacks are Slowloris attacks and ping of death attacks. Slowloris attacks involve sending many packets with a low data rate, resulting in the slow consumption of network resources. The aim of a Slowloris attack is to exhaust the network resources, such as memory and processing power, and to slow down the network performance. slowloris attacks can be generated using tools such as hping or scapy, which allow for the manipulation of packet content and timing. Ping of death attacks involves sending a malformed packet that exceeds the maximum packet size allowed by the network protocol. This can cause the target node to crash or freeze, resulting in a denial of service (DoS) attack. Ping of death attacks can be generated using tools such as ping flood or nmap. To inject intrusion attacks into a WSN, the NS3 simulator can be used, which provides several options for defining the attack parameters. The attack parameters can be defined based on the type of attack being simulated, such as the number of packets, packet size, packet rate, and packet content. The injection of the attack can be scripted to occur at a specific time or triggered by a specific event.

1. Slowloris attack:
1. for k = 1 to K do
2. for i = 1 to N do
3. send packet of size S to node i every T seconds
4. end for
5. wait for D seconds
6. end for

N is the number of nodes in the network.

T is the time interval between packet transmissions.

D is the duration of the attack.

K is the number of connections to be established.

S is the size of the packets to be sent.

2. Ping of Death Attack:

The formula for injecting the Ping of Death attack is:

1. for I = 1 to N do
2. send packet of size P to node I every T second.
3. end for

wait for D seconds

Let N be the number of nodes in the network.

Let T be the time interval between packet transmissions.

Let D be the duration of the attack.

Let P be the size of the packets to be sent.

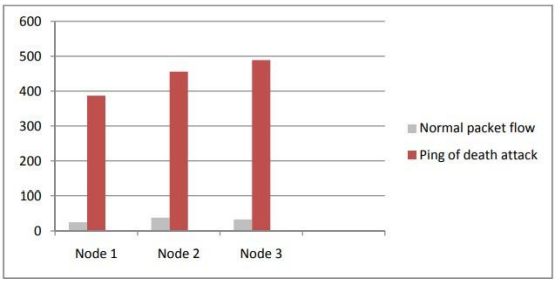

Figure3: Comparison of the Ping of Death attack and typical ICMP packet flow

d. Capturing Packets

Capturing packet traffic is an essential aspect of analysing the performance of a Wireless Sensor Network (WSN) after an intrusion attack has been injected. Packet traffic analysis can provide insights into the impact of the intrusion on network performance, identify the affected nodes, and determine the type of intrusion. After the intrusion attack has been injected into the WSN, the packet traffic can be captured using tools. These tools allow for the capture and analysis of packets flowing through the network. The captured packet traffic can be analyzed to measure performance metrics such as packet delivery ratio, delay, and throughput. The packet traffic can also be used to identify the source and destination of the packets and to determine the types of packets generated. Packet feature extraction is an essential step in analysing packet traffic after an intrusion attack. This involves extracting specific packet features such as packet size, packet rate, packet content, and packet timing. These features can be used to classify the type of intrusion and to identify the affected nodes in the network.

e. Packet Feature Extraction

Packet feature extraction is an essential step in analysing packet traffic in a Wireless Sensor Network (WSN). Packet features are characteristics of a packet that can be used to identify the packet type, source, destination, and content. Packet feature extraction involves extracting specific features from the captured packet traffic, such as packet size, packet rate, packet content, and packet timing. Packet size is a crucial feature of a packet, as it can be used to identify the type of packet generated. For example, a large packet size may indicate a ping of death attack, while a small packet size may indicate a slowloris attack. Packet rate, on the other hand, refers to the frequency at which packets are generated. A high packet rate may indicate an intrusion attack, as the attacker attempts to flood the network with packets to overwhelm it. Packet content is another critical feature that can be extracted from the captured packet traffic. This involves analysing the payload of the packet to identify the information being transmitted. Packet content can be used to identify the type of intrusion and to determine the affected nodes in the network.

f. Classification

Classifying the intrusion type is a crucial step in analysing packet traffic in a Wireless Sensor Network (WSN) after an intrusion attack has been injected. Intrusion detection and prevention mechanisms rely on accurately identifying the type of intrusion to effectively mitigate its impact. Packet feature extraction and machine learning algorithms can be used to classify the intrusion type accurately. Packet features such as packet size, packet rate, packet content, and packet timing can be used as input features to train a machine learning model to classify the intrusion type accurately. The model can be trained using labelled data, where the packets have been classified according to the type of intrusion they represent. Once the model has been trained, it can be used to classify the intrusion type in real-time. The model takes the extracted packet features as input and provides a classification output based on the type of intrusion detected. The classification output can be used to trigger appropriate intrusion detection and prevention mechanisms, such as blocking the attacker's IP address or initiating network reconfiguration.

g. Prevention

Packet Transverse Prevention (PTP) is a prevention method used to protect Wireless Sensor Networks from resource exhaustion attacks. PTP works by monitoring the number of packets sent by each node and blocking those nodes that exceed a predefined threshold. By blocking these nodes, PTP can prevent resource exhaustion and ensure that the network remains available and reliable. PTP operates by analysing packet headers and monitoring packet transmissions in real-time. Nodes that send packets above the predefined threshold are identified and blocked. PTP can also be configured to allow a certain number of packets to be sent before blocking a node, which can help prevent false positives and ensure that legitimate traffic is not blocked.

In addition to blocking nodes, PTP can also be used to prioritize traffic from critical nodes, such as those involved in monitoring environmental conditions or detecting security breaches. This can help ensure that critical data is transmitted without delay and is not impacted by resource exhaustion attacks. Packet Transverse Prevention is an effective method for preventing resource exhaustion attacks in Wireless Sensor Networks. By monitoring packet transmissions and blocking nodes that exceed predefined thresholds, PTP can ensure that the network remains reliable and available, even in the face of persistent attacks.

IV. Workflow

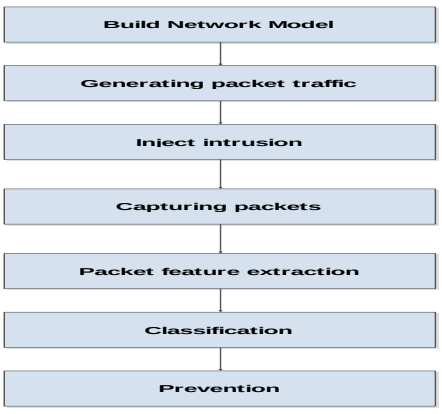

Figure4: Workflow of the project

The overall workflow for preventing intrusion attacks and resource exhaustion in Wireless Sensor Networks involves several steps. First, a network model is built in ns3, followed by the injection of two types of attacks - slowloris and ping of death. Packet traffic is then generated, captured, and analyzed to extract relevant packet features, which are used to classify the type of intrusion. Finally, prevention mechanisms such as delay before and after response and access control are employed to prevent resource exhaustion attacks. By following this workflow, network administrators can effectively detect and prevent attacks, ensuring that the network remains reliable and available.

Algorithm

step1: Number of nodes

step2 :Node creation and started communication (before)

step3: Identifying border and corner nodes

Step4: Directed traffic and undirected traffic moving in network. Regular and uncontrolled traffic communication(After)

```
df = pd.DataFrame({ 'from':rlist, 'to':tolist})
G=nx.from_pandas_edgelist(df, 'from', 'to', create_using=nx.DiGraph() )
nx.draw(G, with_labels=True, node_size=1500, alpha=0.3, arrows=True)
plt.title("Directed")
plt.show()
df = pd.DataFrame({ 'from':rlist, 'to':tolist})
G=nx.from_pandas_edgelist(df, 'from', 'to', create_using=nx.Graph() )
nx.draw(G, with_labels=True, node_size=1500, alpha=0.3, arrows=True)
plt.title("UN-Directed")
plt.show()
```

step5: Calculating nod value, response delay etc for analysis

step6: Graph depicting the behaviour before and after communication

V. Results And Discussion

Using the proposed methodology, network administrators can effectively detect and prevent resource exhaustion attacks in Wireless Sensor Networks. The injection of slow race and ping of death attacks, combined with the analysis of packet traffic, can help identify the type of intrusion and allow for the implementation of prevention methods such as delay before and after response or Packet Transverse Prevention.

The prevention methods proposed in the paper can also help ensure that critical data is

transmitted without delay, even in the face of persistent attacks. By prioritizing traffic from critical nodes and blocking nodes that exceed predefined thresholds, the network can remain reliable and available for its intended purpose.

Overall, the results of the paper suggest that a combination of prevention methods and regular updates and patches to the network infrastructure and devices can help effectively detect and prevent intrusion attacks and resource exhaustion in Wireless Sensor Networks, ensuring that the network remains secure and reliable for its intended use.

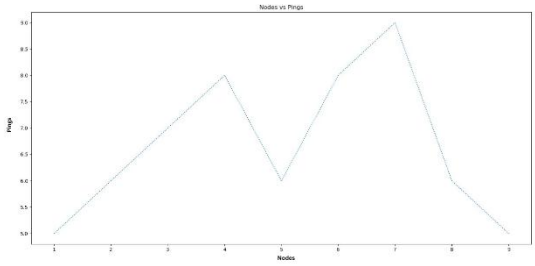

Figure5:Ping of death using ns3

The link between the quantity of nodes in a Wireless Sensor Network (WSN) and the typical number of pings each node receives is shown as a line graph. The graph demonstrates that as the number of nodes rises, so does the average number of pings each node receives. This implies a relationship between the size of the network and the workload of individual nodes. Network administrators can optimise the WSN's design by analysing the graph. They can figure out the ideal number of nodes the network can accommodate without suffering performance degradation. It offers information about the network's capacity and aids managers in finding the right balance between the number of nodes and the workload each one can effectively handle.

The graph also provides information on how WSNs behave in various network sizes. This data can be used by network managers to enhance performance and dependability. Based on the observed trends allocation, load balancing strategies, or network setup. Through this optimisation, the WSN is able to work more dependably and effectively, improving its overall performance.

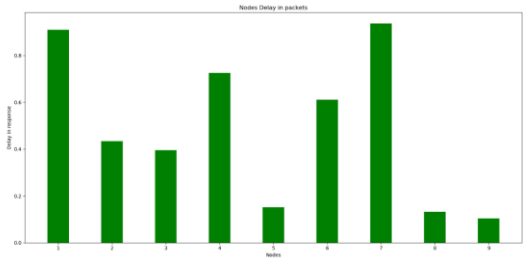

Figure6. Slow loris attack using ns3

The bar graph represents the delay in packets experienced by different nodes in a Wireless Sensor Network. The x-axis represents the node numbers, while the y-axis shows the delay in packets. Each bar in the graph represents the delay in packets experienced by a particular node. The height of the bar indicates the magnitude of delay experienced by that node, with higher bars indicating higher delays. The bar graph can be used to identify nodes that are experiencing high delays and troubleshoot issues related to network congestion or other factors that may be causing delays. It can also inform network administrators on the distribution of delays across the network and assist in optimizing the network performance. Overall, the bar graph provides a visual representation of the delays experienced by different nodes in a Wireless Sensor Network, allowing for targeted analysis and optimization of network performance.

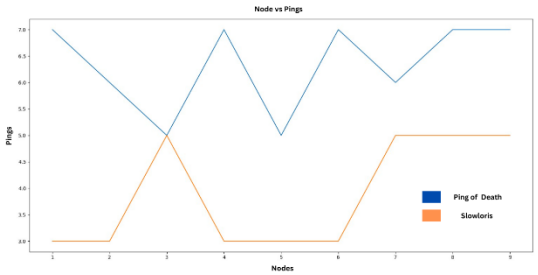

Figure7. Combination of attacks using ns3

The graph shows the delays that take place both before and after the network reacts to the intursion. It is simple to evaluate the variations in delay times between the pre-response and post-response phases .Researchers or network administrators can learn more about the network's overall performance in identifying and defending against various forms of intrusion threats by analysing these delay patterns. The sorts of intrusion that cause lengthy delays after the

network responds are of special interest because they could point to security flaws or vulnerabilities in the network.. In a Wireless Sensor Network, this line graph illustrates the latency before and after reaction for different types of intrusion. It is a useful tool for monitoring the network's reaction time to intrusion attempts, determining the kinds of intrusion that result in substantial delays, and directing security steps to improve the security and effectiveness of the network as a whole.

VI. Conclusion

In conclusion, preventing intrusion attacks and resource exhaustion in Wireless Sensor Networks is crucial to ensure the reliability and availability of the network. In this paper, we have proposed a methodology for preventing resource exhaustion attacks, which includes building a network model, injecting two types of attacks (Slow Loris and ping of death), generating and analysing packet traffic, and classifying the type of intrusion. We have also discussed various prevention methods, including delay before and after response and Packet Transverse Prevention. These methods can effectively prevent resource exhaustion attacks and ensure that critical data is transmitted without delay. Therefore, a combination of prevention methods should be employed to ensure the maximum protection of the network. In addition, regular updates and patches to the network infrastructure and devices should be performed to address newly identified vulnerabilities and ensure that the network is secure. Overall, the methodology and prevention methods proposed in this paper can help network administrators effectively detect and prevent intrusion attacks and resource exhaustion in Wireless Sensor Networks, ensuring that the network remains reliable and available for its intended purpose.

VII. Future Enhancement

Future research in intrusion detection and prevention for resource exhaustion in Wireless Sensor Networks includes creating more sophisticated algorithms, investigating machine learning, examining the effects of network parameters, creating more effective prevention mechanisms, researching blockchain technology, and investigating novel communication protocols. Applications like environmental monitoring, industrial automation, and healthcare all require Wireless Sensor Networks to be more secure and effective.

VIII. References

[1] Kumar, B. S., & Gowda, V. S. (2022, July). Detection and Prevention of UDP Reflection Amplification Attack in WSN Using Cumulative Sum Algorithm. In 2022 IEEE International Conference on Data Science and Information System (ICDSIS) (pp. 1-5). IEEE.

[2] Kumar, B. S., & Gowda, K. K. (2022, July). Detection and Prevention of TCP SYN Flooding Attack in WSN Using Protocol Dependent Detection and Classification System. In 2022 IEEE International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

[3] Kumar, B. S., & Sinha, S. (2022, June). An Intrusion Detection and Prevention System against DOS Attacks for Internet-Integrated WSN. In 2022 7th International Conference on Communication and Electronics Systems (ICCES) (pp. 793-797). IEEE.

[4] Kumar, B. S., & Anaswara, P. P. (2018). Vulnerability detection and prevention of SQL injection. International Journal of Engineering & Technology, 7(2.31), 16-18.

[5] Lakshmi, H. N., Anand, S., & Sinha, S. (2019). Flooding attack in wireless sensor network-analysis and prevention. International Journal of Engineering and Advanced Technology, 8(5), 1792-1796.

[6] Godala, S., & Vaddella, R. P. V. (2020). A study on intrusion detection system in wireless sensor networks. International Journal of Communication Networks and Information Security, 12(1), 127-141.

[7] Desnitsky, V., Kotenko, I., & Zakoldaev, D. (2019). Evaluation of resource exhaustion attacks against wireless mobile devices. Electronics, 8(5), 500.

[8] Rezvi, M. A., Moontaha, S., Trisha, K. A., Cynthia, S. T., & Ripon, S. (2021). Data mining approach to analyzing intrusion detection of wireless sensor network. Indonesian J. Electric. Eng. Comput. Sci, 21(1), 516-523.

[9] Abdollahi, A., & Fathi, M. (2020). An intrusion detection system on ping of death attacks in IoT networks. Wireless Personal Communications, 112, 2057-2070.

[10] Singh, R., Awasthi, L. K., & Sharma, K. P. (2021). Distributed denial-of-service attacks and mitigation in wireless sensor networks. Distributed Denial of Service Attacks: Concepts, Mathematical and Cryptographic Solutions, 6, 67.

[11] Subramani, S., & Selvi, M. (2023). Comprehensive review on distributed denial of service attacks in wireless sensor networks. International Journal of Information and Computer Security, 20(3-4), 414-438.

[12] Sabri, S., Ismail, N., & Hazzim, A. (2021, February). Slowloris DoS attack based simulation. In IOP Conference Series: Materials Science and Engineering (Vol. 1062, No. 1, p. 012029). IOP Publishing.

[13] Panigrahi, R., Borah, S., Pramanik, M., Bhoi, A. K., Barsocchi, P., Nayak, S. R., & Alnumay, W. (2022). Intrusion detection in cyber–physical environment using hybrid Naïve Bayes—Decision table and multi-objective evolutionary featureselection. ComputerCommunications, 188, 133-144.

[14] Owaimer, F. A., Tanira, A., Hatab, M. A., Mikki, M., Fuad, A., Owaimer, A., ... & Hatab, M. M. (2022). An Efficient Intrusion Detection Approach for Wireless Sensor Networks. Authorea Preprints.

[15] Sinha, S. (2021, September). Network layer DoS Attack on IoT System and location identification of the attacker. In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 22-27). IEEE.

[16] Anand, S., & Adithi, B. P. (2022). Detection and Prevention of Faulty Node in Heterogeneous Wireless Sensor Network. In Soft Computing for Security Applications: Proceedings of ICSCS 2021 (pp. 383-397). Springer Singapore.

[17] Shwetha, B., Brunda, I. B., & Sinha, S. (2022, August). Activity Oriented Malicious Node Identification for Packet Drop Attack in WSN. In 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 549-556). IEEE.

[18] Anand, S., & Sinha, S. (2023). Path Generation Protocol to Improve Lifetime of WSN. Procedia Computer Science, 218, 1091-1101.

[19] Acharya, A. A., Arpitha, K. M., & Kumar, B. S. (2016). An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET. International Journal of Engineering and Technology (IJET), 8(2).

[20] Bin, S., & Sun, G. (2020). Optimal energy resources allocation method of wireless sensor networks for intelligent railway systems. Sensors, 20(2), 482.