



doi:10.5281/zenodo.18737972

Assessment Of Machine Learning Technique For Real Time Intrusion And Wormhole Attack Detection In Internet Of Things

Paul Owoicho Gideon, Dr. S.E Chaku, Dr. V.E Kulugh & Prof. M.O. Adenemon

Centre for cyberspace studies, Nasarawa state university, Keffi, Nasarawa State. Nigeria

ABSTRACT

This study investigated the real-time detection of intrusion and wormhole attacks in Internet of Things (IoT) environments using machine learning algorithms. A quantitative survey research design was adopted, employing a structured questionnaire to collect data from 109 respondents. The data were analyzed using SPSS version 27, and the hypotheses were tested with a one-sample t-test. The primary objectives of the study were to examine how machine learning models can improve the detection of attacks compared to traditional methods, evaluate the effectiveness of these models in real-time attack detection, and assess their capacity to adapt to evolving security threats. The findings revealed that machine learning algorithms significantly enhanced the detection of both intrusion and wormhole attacks in IoT networks, offering faster and more accurate results than traditional rule-based methods. Respondents highlighted the superior ability of machine learning models to reduce false positives while maintaining high detection rates. Additionally, the study showed that machine learning models adapted better to emerging threats, such as zero-day attacks, providing stronger protection against advanced persistent threats. These results align with previous research, which has indicated that machine learning offers critical advantages in handling the complex and dynamic nature of IoT security threats. In conclusion, this study provided substantial evidence that machine-learning techniques are essential for improving security in IoT networks. The research supports the notion that real-time attack detection using machine learning algorithms can significantly enhance the security of IoT environments, addressing vulnerabilities that traditional security systems often overlook.

Keywords: Internet of things (IoT), Wormhole attack, Machine learning (ML), supervised learning, Unsupervised learning, Anomaly Detection, False Positive.

1. INTRODUCTION

The Internet of Things (IoT) represents a rapidly growing ecosystem of interconnected devices that communicate and share data through the Internet. This vast network of devices is transforming multiple industries by enabling greater automation and efficiency in sectors such as healthcare, agriculture, transportation, and urban planning (Farjammia, Gasimov, & Kazimov, 2019). IoT technologies allow devices to collect and exchange data seamlessly, optimizing processes and offering real-time solutions to everyday problems. For instance, in agriculture, IoT sensors can monitor soil moisture levels and crop health, while in healthcare, IoT-enabled devices provide continuous patient monitoring, improving diagnosis and treatment (Ghugar & Pradhan, 2020). Despite the many benefits, the expansion of IoT also brings several security challenges, primarily due to the increased connectivity and the growing attack surface of interconnected devices.

One of the most concerning threats to IoT networks is intrusion attacks, which occur when unauthorized users or entities gain access to the IoT network, often for malicious purposes such as the sensitive information or disruption of services (Kumar, 2020). These attacks can exploit vulnerabilities in IoT devices, which often have limited processing power and may not feature advanced security mechanisms. For example, compromised devices can be used to launch attacks on other devices within the network, spreading malicious software or stealing critical data. As the number of connected devices grows, the risk of successful intrusion attacks also increases, posing serious threats to the confidentiality, integrity, and availability of data transmitted through IoT systems.

Another major concern is the threat of wormhole attacks, which are particularly dangerous in mobile ad hoc networks and IoT systems (Giri, Borah, & Pradhan, 2018). In this type of attack, malicious nodes create a "wormhole" by establishing a tunnel between two distant parts of the network. This tunnel allows the attackers to intercept, alter, or even drop communication between legitimate nodes, undermining the trust and reliability of the network. By manipulating or disrupting network traffic, wormhole attacks can cause significant degradation in the performance of IoT systems, making them unreliable for critical applications like healthcare monitoring or autonomous vehicle navigation (Padmapriya, Jeyalakshmi, & Kamalakkannan, 2018). These attacks can also enable further breaches in security, allowing attackers to perform more sophisticated exploits, such as data injection or denial of service attacks.

Traditional security mechanisms, such as firewalls and encryption, are often insufficient in protecting IoT systems from these complex threats. The IoT environment is dynamic and heterogeneous, with devices from different manufacturers, operating on various protocols, and often lacking adequate built-in security features (Memon et al., 2021). Firewalls, while useful in some contexts, are not designed to handle the scale and diversity of IoT networks. Encryption, though crucial for protecting data in transit, can be computationally expensive for resource-constrained IoT devices, leading to performance issues and potential vulnerabilities. Therefore, there is a pressing need for more adaptive and intelligent security solutions that can cope with the unique challenges posed by IoT systems.

Machine learning (ML) has emerged as a powerful tool to address these security challenges in IoT networks (Liu, Dong, Ota, & Liu, 2020). By utilizing ML algorithms, IoT systems can analyze massive amounts of data generated by connected devices in real time. This allows for the detection of abnormal patterns or deviations from the norm, which could indicate the presence of an attack, such as an intrusion or a wormhole attack. For example, ML-based intrusion detection systems (IDS) can identify unusual traffic patterns, enabling the system to flag potential threats before they can cause significant damage (Jamali & Fotohi, 2022). Similarly, ML models can be trained to recognize the telltale signs of wormhole attacks, such as changes in the expected routing behaviour of data packets, allowing for the rapid detection and mitigation of such threats.

The application of ML in real-time attack detection for IoT systems presents several advantages over traditional security mechanisms. First, it allows for the identification of threats based on data-driven insights rather than relying on predefined attack signatures, which can quickly become obsolete as attackers evolve their tactics (Farjammia et al., 2019). This makes ML-based systems more adaptable and capable of identifying previously unknown threats. Second, ML algorithms can continuously learn from new data, improving their accuracy over time and becoming more effective at distinguishing between legitimate activity and malicious behaviour (Ghugar & Pradhan, 2020). This is particularly important in IoT networks, where devices constantly generate new data, and the ability to adapt in real time is critical to maintaining robust security.

Another key benefit of integrating ML into IoT security is the ability to offer a scalable solution that can handle the exponential growth of IoT devices. As the number of connected devices increases, the volume of data generated by these devices also grows, making manual monitoring and analysis impractical (Giri et al., 2018). ML algorithms can automate the process of monitoring and analyzing this data, allowing IoT systems to scale securely without the need for additional human resources or intervention. This level of automation is crucial in applications where rapid detection and response are essential, such as in healthcare monitoring systems or autonomous transportation networks.

while IoT networks offer significant benefits in terms of efficiency and automation across various sectors, they also expose users to a range of security vulnerabilities, including intrusion and wormhole attacks. Traditional security mechanisms often fail to address the unique challenges posed by the heterogeneous and dynamic nature of IoT systems. However, the integration of machine learning into IoT security offers a promising solution, enabling real-time attack detection, adaptive defences, and scalable security mechanisms. As IoT continues to expand and evolve, the application of ML will play a crucial role in safeguarding these networks against the growing array of threats, ensuring that the potential of IoT can be fully realized without compromising security (Memon et al., 2021).

Objectives of the Study

The study aimed to assess machine learning technique for real time intrusion and wormhole attack detection in internet of things. The specific objectives to achieve the above aim are:

1. To Identify and analyze the key characteristics of intrusion and wormhole attacks in IoT networks.
2. To evaluate the potential of machine learning algorithms in detecting intrusion and wormhole attacks in real-time IoT environments.
3. To assess the performance of machine learning techniques, focusing on overall efficiency in real-time IoT scenario.

2. LITERATURE REVIEW

Adil et al. (2020) conducted a quantitative study focusing on an anonymous channel categorization scheme for detecting jamming attacks in Wireless Sensor Networks (WSNs), utilizing simulation models for data analysis. The study revealed that the proposed method significantly enhances the security of edge nodes by effectively identifying and mitigating jamming attacks, thereby improving overall network reliability. By enabling real-time detection of malicious activities, the scheme minimizes the adverse impacts of jamming on data transmission, which is crucial for the functionality of WSNs in applications like environmental monitoring and industrial automation. Additionally, the research highlights the adaptability of the scheme to various WSN applications, reinforcing the need for robust security protocols to counteract evolving cyber threats. The findings underscore the importance of developing real-time detection mechanisms and adaptive response strategies to safeguard wireless sensor systems, aligning with other studies that advocate for advanced security measures in network communications (Sah & Amgoth, 2020; Numan et al., 2020). This approach not only contributes to the resilience of WSNs but also sets a precedent for future research in the field of network security.

Elsayed et al. (2018) adopted a quantitative research design, utilizing simulation-based analysis to propose a self-maintenance model aimed at enhancing energy efficiency, fault tolerance, and scalability in Wireless Sensor Networks (WSNs). Their findings revealed that the model effectively addresses key challenges in maintaining WSNs by ensuring robust performance even in the presence of environmental changes or network failures. The model's adaptive capabilities make it a valuable tool for managing energy resources and extending network lifetime, which is critical in the context of large-scale deployments. By autonomously adjusting to operational faults, the model minimizes the need for human intervention, ensuring continuous and reliable sensor data collection. Furthermore, the study highlights the necessity of scalable solutions to accommodate the growing demands of WSNs in smart city applications and industrial monitoring (Sah & Amgoth, 2020; Numan et al., 2020). The implications of this research suggest that incorporating self-maintenance capabilities into WSNs can significantly reduce operational costs and enhance the longevity of sensor networks, positioning it as a key advancement in the field of wireless sensor security and network resilience.

Sah and Amgoth (2020) employed a qualitative research design, conducting a comprehensive survey on renewable energy harvesting schemes for Wireless Sensor Networks (WSNs). Their findings highlighted several energy harvesting mechanisms such as solar, vibration, and thermal energy, which are vital for sustaining long-term WSN operations. The study revealed that renewable energy sources could significantly alleviate the constraints of battery limitations, making WSNs more sustainable in remote and off-grid

applications. By incorporating renewable energy harvesting technologies, WSNs can function autonomously for extended periods without frequent maintenance or battery replacements. This advancement is especially crucial for large-scale deployments in environments such as smart cities, agriculture, and industrial monitoring, where the cost of energy supply and sensor maintenance can be prohibitive (Elsayed et al., 2018; Numan et al., 2020). Furthermore, the study emphasized that optimizing energy harvesting schemes for different environmental conditions could improve network performance and reduce operational costs. The implications of this research underscore the importance of integrating renewable energy solutions into WSNs to enhance their scalability, operational efficiency, and sustainability in modern sensor-based applications.

Sampoornam et al. (2021) employed a quantitative research design, analyzing the vulnerabilities of the LEACH routing protocol to wormhole attacks in Wireless Sensor Networks (WSNs) using simulations and data analysis techniques. Their study revealed that wormhole attacks significantly disrupt the normal operations of the LEACH protocol, compromising data integrity and network functionality. The study showed that the malicious introduction of false routing information could lead to the misrouting of packets, which increases energy consumption and degrades the overall performance of the WSN. Additionally, the researchers found that the security weaknesses in the LEACH protocol made it highly susceptible to such attacks, emphasizing the need for enhanced security mechanisms to safeguard routing protocols in WSNs. These findings underscore the importance of securing routing protocols to ensure the reliability and security of data transmission in WSNs, especially in mission-critical applications such as military surveillance and environmental monitoring (Wang et al., 2020). The implications of this study suggest that future research should focus on designing more resilient routing protocols or integrating security measures such as cryptographic techniques to protect against wormhole attacks, thereby improving the robustness of WSNs in hostile environments.

Shahraki et al. (2020) conducted a survey using a qualitative research design to examine clustering objectives in Wireless Sensor Networks (WSNs), focusing on cluster formation challenges in large networks. Their analysis revealed that the process of forming clusters in WSNs is significantly affected by network scalability, where larger networks tend to encounter difficulties in maintaining effective and balanced clustering. The study emphasized the need for more advanced clustering techniques that can address both the energy efficiency and the scalability concerns of WSNs. Additionally, the researchers found that traditional clustering methods struggle to optimize energy consumption, especially as the network grows, leading to premature node exhaustion and reduced network lifetime. Their findings highlight the critical role of efficient clustering mechanisms in prolonging network operations and ensuring the scalability of WSNs. The implications suggest that future research should focus on designing adaptive clustering algorithms that can dynamically respond to the network size and environmental conditions, thus enhancing the overall energy efficiency and performance of WSNs

3. METHODOLOGY

3.1 Research Design

The research design for this study is a **quantitative survey** approach, which was selected for its ability to gather numerical data that can be statistically analyzed. A survey design allows the researcher to collect data from a large group of respondents, enabling generalization of results to the broader population (Creswell & Creswell, 2018; Saunders et al., 2019). This design is particularly suitable when the objective is to examine relationships between variables and to obtain data that are quantifiable and objective. A structured questionnaire was developed to gather specific responses on the topic of Real time intrusion and wormhole attacks detection in internet of thing using machine learning. This design also facilitates the collection of standardized data, making it easier to perform statistical tests such as correlations, t-tests, and regression analysis, which are commonly used to explore patterns and relationships in large data sets (Bell et al., 2019).

3.2 Population of the Study

The population of a study refers to the complete set of individuals or elements that share specific characteristics and are the subject of a research investigation (Frankfort-Nachmias, Nachmias, & DeWaard, 2021). In this study, the target population consisted of 1200 respondents. The selection of this population is based on the scope of the study and the relevance of the participants to the research objectives. These individuals were chosen because they represent the demographic of interest in the context of the research. The target population's characteristics align with the study's focus, ensuring the responses gathered will provide valuable insights into the subject matter.

The decision to select this population was also influenced by the study's goal of obtaining a representative sample that could provide reliable data for the research. The size of the population is large enough to ensure that a diverse range of opinions and behaviors could be captured. Moreover, having a target population of this size increases the reliability and validity of the research findings.

3.2.1 Sampling Technique and Sample Size

Sampling is the process of selecting a subset of individuals from a larger population to participate in a study. The sample size and the sampling technique are crucial for ensuring the representativeness of the sample and the accuracy of the findings (Charan & Biswas, 2019). In this study, purposive sampling was adopted. Purposive sampling, also known as judgmental sampling, involves selecting participants based on specific characteristics or qualities that are relevant to the research objectives (Saunders, Lewis, & Thornhill, 2019). This non-random technique was deemed appropriate because it allowed the researcher to target individuals who have the necessary knowledge or experience related to the research topic, ensuring the sample's relevance and quality.

A sample size of 120 respondents was selected, representing 10% of the target population. This sample size is justified by the need to balance between feasibility and reliability. According to Sreedharan, Chandrasekharan, and Gopakumar (2019), selecting a sample that is about 10% of the total population is often considered an optimal size for ensuring both a manageable workload and sufficient data to draw meaningful conclusions. By adopting a purposive sample of 120 individuals, the study aimed to achieve both depth and breadth in the data collected, focusing on those respondents who are directly relevant to the research.

3.3 Methods of Data Collection

Data for this study were collected using a **structured questionnaire**. The questionnaire was designed to capture data related to Real time intrusion and wormhole attacks detection in internet of thing using machine learning, with sections addressing the key research questions. Structured questionnaires are beneficial because they ensure consistency in the questions asked, making the data easier to quantify and analyze (Morse et al., 2022).

The questionnaire was administered in both **paper** and **digital formats** to maximize reach and participation. Digital formats, such as online surveys, were utilized to ensure the study's inclusivity and to facilitate the collection of data from a broader geographic area (Gray, 2018). Participants were informed about the purpose of the study and assured of confidentiality and voluntary participation, which helped to ensure ethical standards (Tavakol & Dennick, 2021).

3.4 Technique for Data Analysis

Data analysis for this study was conducted using **SPSS 27 (Statistical Package for the Social Sciences)**. SPSS is a widely used statistical software that allows for efficient handling and analysis of large datasets (Gray, 2018). The data collected from the questionnaires were entered into SPSS, where both **descriptive and inferential statistics** were applied.

Descriptive statistics, such as frequencies, means, and percentages, were used to summarize the characteristics of the respondents and provide an overview of the collected data. **Inferential statistics** such as **t-tests**, were used to determine relationships between key variables, test hypotheses, and make inferences about the population based on the sample data (Frankfort-Nachmias et al., 2021). These methods were chosen because they allow for the determination of statistically significant relationships, as well as the testing of research hypotheses (Creswell & Creswell, 2018).

3.5 Justification of Methods

The use of a **quantitative research design** is justified due to the need for objective measurement and statistical analysis to draw reliable conclusions about the research questions. Quantitative data collection through structured questionnaires ensures the reliability and consistency of responses, allowing for generalizability across the study population (Creswell & Creswell, 2018).

The **purposive sampling technique** was appropriate for this study because it allowed for the selection of participants who had direct experience or knowledge relevant to the research problem, thus ensuring that the data gathered was rich and relevant (Saunders et al., 2019).

The application of **SPSS 27** for data analysis further ensures accuracy and efficiency in handling large datasets. By using a combination of **descriptive** and **inferential statistics**, the study can both summarize the data and make valid inferences about the population, thus addressing the research objectives in a statistically rigorous manner (Charmaz, 2016; Bernard & Ryan, 2019)

DATA ANALYSIS AND RESULTS

Table 4.1: Distribution of Questionnaire

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Returned/Completed	109	90.8	90.8	90.8
	Not Returned/Uncompleted	11	9.2	9.2	100.0
	Total	120	100.0	100.0	

Source: SPSS27 Output, 2024

4.1.1 Demographic Data of Respondents

Table 4.2: Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	46	42.2	42.2	42.2
	Female	63	57.8	57.8	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

The gender distribution of the respondents, as shown in Table 4.2, reveals that the sample consisted of 46 male participants (42.2%) and 63 female participants (57.8%). This indicates a higher proportion of female respondents compared to male participants. The higher representation of females may suggest that the topic of IoT security and intrusion detection resonates more with women in this study, or it could be reflective of the gender makeup of the research population.

Table 4.3: Age Range

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24 years	17	15.6	15.6	15.6
	25-34 years	78	71.6	71.6	87.2
	35-44 years	8	7.3	7.3	94.5
	45 years and above	6	5.5	5.5	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

The age distribution of respondents, as presented in Table 4.3, highlights that the majority of participants (71.6%) were between the ages of 25-34 years. This is a significant portion of the sample, suggesting that this age group is more engaged with the topic of IoT security and intrusion detection.

Table 4.4: Educational Attainment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bachelor's degree	8	7.3	7.3	7.3
	Master's degree	65	59.6	59.6	67.0
	Others	36	33.0	33.0	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

The educational attainment of respondents, as shown in Table 4.4, indicates that a substantial portion of participants (59.6%) held a Master's degree. This suggests that the study attracted a highly educated group of individuals, which is typical in research involving technical topics such as IoT security. Individuals with a higher level of education are likely to have a better understanding of complex concepts related to cybersecurity, machine learning, and intrusion detection, making them well-suited to contribute to this research. Their involvement adds depth to the findings, as their responses are likely to be informed by advanced knowledge and professional experience in relevant fields.

Table 4.5: Professional Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5 years	6	5.5	5.5	5.5
	6-10 years	36	33.0	33.0	38.5
	More than 10 years	67	61.5	61.5	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

The professional experience of respondents, as shown in Table 4.5, reveals that the majority of participants (61.5%) had more than 10 years of professional experience. This indicates a high level of expertise and familiarity with the field, which is beneficial in understanding complex issues related to intrusion and wormhole attacks in IoT networks. These respondents likely bring a wealth of practical knowledge, offering insights grounded in years of working in areas such as cybersecurity, IoT infrastructure, or related sectors. Their input is invaluable, as individuals with more extensive experience tend to have a broader perspective on challenges and solutions, which can significantly contribute to the study's findings.

Table 4.5: Professional Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5 years	6	5.5	5.5	5.5
	6-10 years	36	33.0	33.0	38.5
	More than 10 years	67	61.5	61.5	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

The professional experience of respondents, as shown in Table 4.5, reveals that the majority of participants (61.5%) had more than 10 years of professional experience. This indicates a high level of expertise and familiarity with the field, which is beneficial in understanding complex issues related to intrusion and wormhole attacks in IoT networks. These respondents likely bring a wealth of practical knowledge, offering insights grounded in years of working in areas such as cybersecurity, IoT infrastructure, or related sectors. Their input is invaluable, as individuals with more extensive experience tend to have a broader perspective on challenges and solutions, which can significantly contribute to the study's findings.

Table 4.6: Technical Expertise in IoT Security:

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Novice	5	4.6	4.6	4.6
	Intermediate	33	30.3	30.3	34.9
	Advanced	71	65.1	65.1	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

The data in Table 4.6, which addresses the respondents' technical expertise in IoT security, shows that a substantial majority (65.1%) of respondents considered themselves to have advanced expertise in the field. This indicates that the majority of participants possess a high level of technical knowledge and skill in IoT security, which is particularly valuable for the study. Such expertise is likely to provide deeper insights into the intricacies of intrusion and wormhole attacks in IoT networks and how machine learning techniques can be applied to detect and mitigate these threats.

4.2 DATA ANALYSIS AND RESULTS

4.2.1 Data Analysis on Research Question 1: What are the key characteristics and patterns of intrusion and wormhole attacks in IoT networks?

Table 4.8: The key characteristics of intrusion attacks in IoT networks include unauthorized data access and malicious control over devices.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SA	53	48.6	48.6	48.6
	A	31	28.4	28.4	77.1
	SD	14	12.8	12.8	89.9
	D	7	6.4	6.4	96.3
	U	4	3.7	3.7	100.0
	Total	109	100.0	100.0	

Source: SPSS27 Output, 2024

Table 4.8 shows that a significant majority of respondents acknowledge the key characteristics of intrusion attacks in IoT networks, specifically unauthorized data access and malicious control over devices. The data reveals that 48.6% of respondents strongly agree (SA) with this statement, and 28.4% agree (A), making up a combined total of 77.1% of participants who affirm that these are critical characteristics of intrusion attacks. This response strongly supports the notion that unauthorized access and malicious control are significant threats to the integrity and security of IoT systems. Given the decentralized and interconnected nature of IoT devices, unauthorized access can lead to severe security breaches, including data theft and control over IoT devices for malicious purposes. These concerns are echoed in existing literature, which highlights unauthorized access and control as primary attack vectors in IoT environments.

On the other hand, 12.8% of respondents strongly disagree (SD), and 6.4% disagree (D) with the statement, suggesting a minority that does not fully recognize these characteristics as primary threats. This may indicate varying levels of understanding or expertise regarding the specific risks associated with IoT security, or perhaps a perception that other attack types are more prominent in their experience.

Additionally, 3.7% of respondents were uncertain (U), reflecting some ambiguity or lack of clarity about the nature of intrusion attacks in IoT networks. This level of uncertainty could point to a need for further

education and awareness, particularly for respondents who may not have direct exposure to the technical aspects of IoT security.

Overall, the responses from the majority align with the widely accepted understanding that unauthorized data access and malicious control are key characteristics of intrusion attacks in IoT networks. This reinforces the need for robust security mechanisms to protect against these types of attacks, emphasizing the importance of securing access to devices and ensuring that malicious control is prevented. The findings highlight the relevance of these issues in current IoT security research and underscore the importance of focusing on these areas for improving the overall security posture of IoT systems.

Table 4.23: One-Sample Test

	T	Df	Sig. (2-tailed)	Test Value = 0	
				Mean Difference	95% Confidence Interval of the Difference
				Lower	Upper
The key characteristics of intrusion and wormhole attacks in IoT networks.	32.267	3	.000	85.75000	77.2925 94.2075
The potential of machine learning algorithms in detecting intrusion and wormhole attacks in real-time IoT environments.	26.081	3	.000	83.50000	73.3112 93.6888
Machine learning-based model for the detection of intrusion and wormhole attacks tailored to IoT systems.	35.315	3	.000	85.7500	78.023 93.477
The performance of the proposed machine learning model, focusing on detection accuracy, rate of false positives, and overall efficiency in a real-time IoT scenario.	18.158	3	.000	86.25000	71.1334 101.3666

Source: SPSS27 Output, 2024

Table 4.23 presents the results of a one-sample test for the key characteristics of intrusion and wormhole attacks, and the potential and performance of machine learning algorithms in detecting and addressing these attacks in real-time IoT environments. All of the t-tests conducted show highly significant results ($p < .001$), with mean differences well above zero, indicating strong agreement with the effectiveness of machine learning in tackling these challenges.

For example, the key characteristics of intrusion and wormhole attacks in IoT networks show a mean difference of 85.75, with a 95% confidence interval ranging from 77.29 to 94.21. This reflects a very strong consensus that the identified characteristics are relevant for understanding the attacks in the context of IoT. Similarly, when assessing the potential of machine learning algorithms in detecting these attacks in real-time, a mean difference of 83.5 (confidence interval: 73.31 to 93.69) underscores the strong belief in machine learning's capability in this area.

The proposed machine learning model tailored for detecting intrusion and wormhole attacks also demonstrates a high mean difference of 85.75, indicating its perceived effectiveness in real-time IoT systems. Lastly, the performance of the proposed model, particularly regarding detection accuracy, false positives, and overall efficiency, shows a mean difference of 86.25 (confidence interval: 71.13 to 101.37), reinforcing the strong support for machine learning as a viable tool for real-time attack detection in IoT networks.

4.2.1 Test of Hypotheses

The one-sample t-test was conducted with an assumed mean of 0, a critical table value of 2.92 at the 5% level of significance, to test the following hypotheses.

For the first hypothesis, H_1 , which posited that machine learning algorithms significantly improve the detection of intrusion attacks in IoT networks compared to traditional detection methods, the test result showed a t-value of 32.267 and a mean difference of 85.75 (with a confidence interval between 77.29 and 94.21). Since the calculated t-value far exceeded the critical value of 2.92 and the p-value was less than 0.05, we rejected the null hypothesis. This indicated that machine learning algorithms significantly improve the detection of intrusion attacks in IoT networks compared to traditional methods.

In testing the second hypothesis, H_2 , which suggested that machine learning algorithms significantly improve the detection of wormhole attacks in IoT networks compared to traditional detection methods, the test result again showed a t-value of 26.081 and a mean difference of 83.5 (confidence interval from 73.31 to 93.69). The calculated t-value was also much higher than the critical value, and the p-value was well below 0.05, leading to the rejection of the null hypothesis. This confirmed that machine learning algorithms significantly improve the detection of wormhole attacks in IoT networks compared to traditional methods.

For the third hypothesis, H_3 , which proposed that machine learning-based models provide higher detection accuracy and lower false positive rates in real-time attack detection than traditional security mechanisms in IoT networks, the t-test revealed a t-value of 35.315 with a mean difference of 85.75 (confidence interval ranging from 78.02 to 93.48). The t-value again exceeded the critical value of 2.92, and the p-value was significantly below 0.05, leading to the rejection of the null hypothesis. Therefore, it was concluded that machine learning-based models provide higher detection accuracy and lower false positive rates in real-time attack detection compared to traditional security mechanisms in IoT networks.

4.3 DISCUSSION OF FINDINGS

The findings of this study align closely with the existing literature, underscoring the critical role that machine learning (ML) algorithms play in enhancing the detection of both intrusion and wormhole attacks in IoT networks. Machine learning's ability to outperform traditional security methods in terms of accuracy, efficiency, and real-time response times is well-documented in previous studies, and the findings from this study further reinforce this view.

One of the primary findings of this study is that machine learning significantly improves the detection of intrusion and wormhole attacks in IoT networks. This result is consistent with the literature that emphasizes machine learning's capacity to adapt and evolve in response to emerging threats. For instance, previous studies have shown that traditional security mechanisms, like rule-based systems, struggle to keep up with sophisticated attacks such as wormhole attacks, which exploit IoT network vulnerabilities without leaving obvious traces (Zhou et al., 2020; Ahmad et al., 2019). Machine learning models, on the other hand, have been proven to efficiently detect these types of attacks by learning from large datasets and identifying anomalies that traditional methods often miss (Nguyen & Kim, 2021). This study's finding that machine learning models are able to detect both intrusion and wormhole attacks in real time aligns with the work of Liu et al. (2019) who noted that machine learning, especially in IoT environments, offers superior detection capabilities, particularly in complex attack scenarios.

Another key finding is that machine learning models reduce false positives while improving detection accuracy. Traditional intrusion detection systems often generate a high number of false positives, which can overwhelm system administrators and detract from their ability to respond to actual threats (Buczak & Guven, 2016). This issue was reflected in the findings, which showed that machine learning-based models had lower false positive rates and higher accuracy in detecting real-time attacks, compared to their traditional counterparts. Several studies, including those by Wu et al. (2020) and Sharma et al. (2021), have highlighted this advantage of machine learning. These studies demonstrated that machine learning algorithms, particularly those using supervised learning models like decision trees and neural networks, are better at distinguishing

benign activities from malicious ones, thus reducing unnecessary alerts and improving the overall effectiveness of the intrusion detection system.

The real-time performance of machine learning models, as found in this study, is another critical advantage over traditional security methods. The ability to process and respond to threats in real-time is essential in IoT environments where devices operate continuously and are highly vulnerable to attacks. As indicated by previous research, machine learning's ability to provide timely responses to attacks is crucial for mitigating potential damage in real-time (Ali et al., 2020; Sharma et al., 2021). The findings of this study are aligned with the research by Ali et al. (2020), who emphasized that machine learning algorithms can process large amounts of data more rapidly than rule-based systems, thereby enhancing response times and making them more effective in real-time threat detection.

Moreover, the study highlights the ability of machine learning-based models to adapt to evolving threats, such as zero-day attacks, more efficiently than traditional methods. This adaptability is critical in IoT networks where the threat landscape is constantly changing. The theoretical framework supporting this adaptability is rooted in the ability of machine learning to continuously learn from new data and adjust its detection capabilities accordingly (Buczak & Guven, 2016; Liu et al., 2019). Previous studies have shown that traditional security systems, which rely on fixed attack signatures, cannot keep up with the rapid evolution of cyber threats. Machine learning, on the other hand, can identify previously unseen attack patterns by continuously adapting its detection mechanisms (Zhou et al., 2020; Ahmad et al., 2019). The findings of this study reinforce this concept by showing that machine learning algorithms, through their adaptive nature, provide better protection against evolving threats in IoT networks, including zero-day attacks.

In essence, the findings of this study align closely with previous research, emphasizing the advantages of machine learning algorithms in detecting and mitigating intrusion and wormhole attacks in IoT networks. The ability of machine learning models to improve detection accuracy, reduce false positives, respond in real-time, and adapt to evolving threats makes them a superior choice compared to traditional detection methods. These findings are in agreement with a wide body of literature that advocates for the integration of machine learning in cybersecurity systems, particularly in the context of IoT networks, where the complexity and scale of operations present significant challenges to traditional security methods

5.2 CONCLUSION

Based on the results from the hypotheses tested, it can be concluded that machine learning algorithms significantly enhance the detection of both intrusion and wormhole attacks in IoT networks, as compared to traditional detection methods. The findings from the one-sample t-tests indicated that the machine learning models achieved a significantly higher mean difference than the assumed mean of 0, confirming their effectiveness in identifying and responding to these attacks in real-time. The critical t-values at a 5% level of significance supported the rejection of the null hypotheses, affirming the superiority of machine learning techniques in comparison to traditional security methods.

The results also highlight that machine learning models not only improve detection accuracy but also reduce false positives, which are a significant challenge in traditional detection systems. The findings show that these models adapt better to new, evolving threats such as zero-day attacks, which traditional methods often fail to identify due to their reliance on predefined signatures. Furthermore, the ability of machine learning models to process data in real-time ensures faster detection and response times, a key factor in mitigating potential damages caused by intrusions and wormhole attacks.

Overall, the study confirms the potential of machine learning in enhancing the security of IoT networks by providing accurate, adaptable, and efficient threat detection. This finding aligns with previous research, which has consistently shown that machine learning algorithms, especially those tailored for network security, can outperform traditional methods in terms of accuracy, scalability, and adaptability. The results underscore the growing need for integrating advanced machine learning techniques into IoT security systems to effectively address the increasingly sophisticated and dynamic nature of cyber threats in these environments.

REFERENCES

- Adil, M., Almaiah, M. A., Alsayed, A. O., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors*, 20(7), 2311. <https://doi.org/10.3390/s20072311>.
- Ahutu, O. R., & El-Ocla, H. (2020). Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. *IEEE Access*, 8, 63270–63282. <https://doi.org/10.1109/ACCESS.2020.2981015>.
- Alenezi, F. A., Song, S., & Choi, B. Y. (2021). WAND: Wormhole attack analysis using the neighbor discovery for software-defined heterogeneous Internet of Things. In *Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1–6). Montreal, QC, Canada: IEEE. <https://doi.org/10.1109/ICCWorkshops50385.2021.9463035>.
- Ali, A., Ming, Y., Chakraborty, S., & Iram, S. (2017). A comprehensive survey on real-time applications of WSN. *Future Internet*, 9(4), 77. <https://doi.org/10.3390/fi9040077>.
- Bell, E. (2022). *Business research methods*. Oxford University Press.
- Bell, E., Bryman, A., & Harley, B. (2019). *Business research methods* (5th ed.). Oxford University Press.
- Bernard, H. R., & Ryan, G. W. (2019). *Analyzing qualitative data: Systematic approaches*. SAGE Publications.
- Charan, J., & Biswas, T. (2019). How to calculate sample size for different study designs in medical research? *Indian Journal of Psychological Medicine*, 35(2), 121–126. <https://doi.org/10.4103/0253-7176.116232>
- Charmaz, K. (2016). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage Publications.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed method approaches* (5th ed.). SAGE Publications.
- Dwivedi, R. K., Sharma, P., & Kumar, R. (2018). Detection and prevention analysis of wormhole attack in a wireless sensor network. In *Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 727–732). Noida, India: IEEE. <https://doi.org/10.1109/Confluence.2018.8442402>.
- Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2018). *Management and business research*. Sage Publications.
- Eisenhardt, K. M. (2015). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550.
- Elsayed, W., Elhoseny, M., Sabbeh, S., & Riad, A. (2018). Self-maintenance model for wireless sensor networks. *Computers and Electrical Engineering*, 70, 799–812. <https://doi.org/10.1016/j.compeleceng.2018.06.008>.
- Farjamnia, G., Gasimov, Y., & Kazimov, C. (2019). Review of the techniques against wormhole attacks on wireless sensor networks. *Wireless Personal Communications*, 105, 1561–1584. <https://doi.org/10.1007/s11277-019-06517-0>.
- Frankfort-Nachmias, C., Nachmias, D., & DeWaard, J. (2021). *Research methods in the social sciences* (8th ed.). Worth Publishers.
- Ghugar, U., & Pradhan, J. (2020). Survey of wormhole attack in wireless sensor networks. *Computer Science and Information Technology*, 2, 33–42. <https://doi.org/10.36548/csit.2020.2.010>.
- Giri, D., Borah, S., & Pradhan, R. (2018). Approaches and measures to detect wormhole attack in wireless sensor networks: A survey. In *Advances in Communication Devices and Networking* (pp. 855–864). Springer. https://doi.org/10.1007/978-981-10-6517-2_88.
- Goddard, W., & Melville, S. (2020). *Research methodology: An introduction* (2nd ed.). Blackwell Publishing.
- Goyal, M., & Dutta, M. (2018). Intrusion detection of wormhole attack in IoT: A review. In *Proceedings of the 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)* (pp. 1–5). Kottayam, India: IEEE. <https://doi.org/10.1109/ICCSDET.2018.00006>.
- Gray, D. E. (2018). *Doing research in the real world* (3rd ed.). Sage Publications.

- Jamali, S., & Fotohi, R. (2022). Defending against wormhole attack in MANET using an artificial immune system. *New Review of Information Networking*, 21, 79–100. <https://doi.org/10.1080/13614576.2021.1951350>.
- Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: An up-to-date survey. *Applied Systems Innovation*, 3(1), 14. <https://doi.org/10.3390/asi3010014>.
- Khidzir, K. A. M., Ismail, N. Z., & Abdullah, A. R. (2018). Validity and reliability of instrument to measure social media skills among small and medium entrepreneurs at Pengkalan Datu River. *International Journal of Development and Sustainability*, 7(3), 1026–1037. Retrieved from <http://www.isdsnet.com/ijds>
- Kumar, S. S. (2020). *Abridgement and prevention of wormhole attack in mobile ad hoc networks using coordinator node* (PhD thesis, Vels University, Chennai, India). Available at: <http://hdl.handle.net/10603/274578>.
- Liu, Y., Dong, M., Ota, K., & Liu, A. (2020). ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 11, 2013–2027. <https://doi.org/10.1109/TIFS.2020.2978424>.
- Liu, Y., Ma, M., Liu, X., Xiong, N. N., Liu, A., & Zhu, Y. (2018). Design and analysis of probing route to defence sinkhole attacks for Internet of Things security. *IEEE Transactions on Network and Service Management*, 7(4), 356–372. <https://doi.org/10.1109/TNSM.2018.2830521>.