Evaluating Security Mechanisms for Wireless Sensor Networks in IoT and IIoT

Tamara Zhukabayeva [1], Atdhe Buja [2*], Melinda Pacolli [3]
[1, 2] International Science Complex "ASTANA", Astana 010000, Eurasian National University, Kazakhstan
[2] ICT Academy Research, Prishtina, Kosovo
[3] Department of Computer Science, University for Business and Technology, Prishtina, Kosovo
Email: [1] t.zhukabayeva@astanait.edu.kz, [2] atdhe.buja@hotmail.com, [3] pacollimelinda@gmail.com
*Corresponding Author

***Abstract*—In the era of interconnected digital ecosystems, the security of Wireless Sensor Networks (WSN) emerges as a pivotal concern, especially within the domains of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT). However, the very nature of WSNs—being distributed, resource-constrained, and often deployed in unattended environments—poses unique cybersecurity challenges. A main issue and challenge remains their Cybersecurity in communication. In this paper, we provide a systematic review focused on three themes including 1) techniques for secure communication in WSN; 2) algorithms and methods for intrusion detection in WSN; and 3) IoT and IIoT security concerning WSN. It has provided the results of its own for the publications made in the data analysis of three themes. The paper also has a simulation experiment to investigate the behavior of WSNs under sinkhole attacks—one of the prevalent threats to network integrity. Utilizing the Contiki OS Cooja simulator, the experiment carefully evaluates the performance of existing detection algorithms and introduces a novel method for identifying and neutralizing malicious nodes. Our simulation discloses unconventional communication patterns during sinkhole attacks running RPL protocol, emphasizing the effectiveness of our detection mechanisms against cyber threats. Particularly, the introduction of a malicious node (Node 13) significantly disrupted network communication, with traditional security mechanisms failing to immediately detect and isolate the threat. The scope of future research work will include the broader spectrum of cyber threats beyond sinkhole attacks, exploring advanced detection mechanisms, and machine learning-based security protocols for enhanced trust and transparency in WSN communications.**

Keywords*—*Wireless Sensor Network; Cybersecurity; Sinkhole Attack Detection; Real-Time Attack Identification; IoT.

I. INTRODUCTION

Wireless Sensor Networks (WSN) have become an essential factor in technological infrastructure developments, enabling innovative applications in diverse fields of industry, environmentalism, healthcare, smart cities, and industrial automation. As these networks of sensors remain and lead us forward, their Cybersecurity and security, in general, is a fundamental need. Threats and cyber-attacks on WSNs can cause disruption of industry operations, data theft, and even physical consequences in some areas where they are applied.

Recent studies have gone further into the analysis of complexity that tries to identify and provide countermeasures to cyber-attacks on WSNs. Research has examined the potential, and the role of fuzzy set logic based on advancing the detection in accuracy and stability in the identification of cyber-attacks in these networks [1]. Another research examination, on the importance of network security, underlines the complexity of providing privacy and security at a time when the great growth of connected devices has brought many challenges for researchers [2]. The research contribution of our study foundation has a particular focus on sinkhole attacks in the domain of WSN security. This study employs a dual-method approach: a thorough literature review coupled with simulation experiments. First, it provides a view of the current cybersecurity measures employed in WSN, identifying limitations and areas for enhancement. Second, through simulation-based experimentation, it provides valuable results in the practical application and potential enhancement of detection techniques, serving as the foundation for future studies at strengthening protection against various cyber threats. Moreover, the application of the Internet of Things (IoT) and Industrial IoT (IIoT) in the industry brought focus to the investigation of actual Cybersecurity countermeasures. An evaluation case study of Cybersecurity enhancements needed for Industrial IoT systems provides information on potential vulnerabilities and countermeasures that can be applied to WSNs, given the interconnectedness of these domains [3]. In the continuity of the elaboration of studies, we can state that the evolution of threats and cyber-attacks has scaled up in the advancement of the methods and techniques employed. In addressing the critical cybersecurity challenges facing Wireless Sensor Networks (WSN) within IoT and IIoT ecosystems, this study presents a thorough analysis and empirical investigation into the effectiveness of adaptive intrusion detection mechanisms against sinkhole attacks.

II. PROBLEM DEFINITION AND RESEARCH QUESTIONS

Continuous works have focused on improving various components such as encryption techniques, developing intrusion detection systems, and establishing trust-based mechanisms to defend sensor data. Regardless of the advances that have been made, the focus on security remains a challenge. While the distribution of WSNs has increased in size and complexity, in various application areas, the challenge of maintaining security as a single-package solution remains. The dominant gap is the constant challenge to provide security if we do not interfere with or disrupt the operations of these networks and sensors that are there. Additionally, we need to comprehend the new vectors of

WSNs vulnerabilities that are being introduced in every emerging technological development, and more broadly in IoT. More specifically, there is a need to address these challenges, and further research into countermeasures to protect WSNs and IoT.

Said that, we want this research to answer two main questions:

1) How is enhancing the Cybersecurity of WSN relevant to the overall security of IoT and IIoT?

2) How can the techniques for secure communication and algorithms for intrusion detection in WSN nodes illuminate security issues?

III. Methodology

Having two different types of questions to answer implies two different methodologies to be used, and we can say we will divide the research into two parts. The first part of the research will focus on a literature review, from where we will discover if securing WSN is indeed relevant to IoT and IIoT security. We will use systematic review also to identify different techniques and algorithms, which will later serve as a basis for the second part of the research, which is the experimental simulation of the identified techniques and algorithms to be able to answer the second question of how those techniques and methods can illuminate any security issue at all. Further down in this paper, the reader will find all the discussions and results divided into two parts, followed by the summarized conclusion on the research results at the end.

IV. Research Part I –Literature Review

This section describes in detail the systematic review conducted focused on 1) techniques for secure communication in WSN; 2) algorithms and methods for intrusion detection in WSN; and 3) IoT and IIoT security concerning WSN. It has provided the results of its own for the publications made in the data analysis of three themes. By utilizing systematic review, the research contributes to findings on the manifestation of technologies and shows the common relation between them.

The research work conducted is based on the methods of literature review following the preferred items for systematic reviews, which have been selected properly to examine and analyze the selected literature about Wireless Sensor Networks (WSN) and techniques for identifying attacks and assessing their security. The articles, and studies which were required to be examined were those related to WSNs and techniques for identifying attacks and assessing their security. These techniques, or new approach models include identifying attacks and assessing the security of WSNs as well as IoT infrastructure. The sources of information in the articles were found by searching on the Internet. As a complete landscape, and further, the idea was established by examining actual examples as well as focusing on relevant articles from scientific sources. We searched databases like IEEE, Elsevier, and ACM DL for articles on WSNs and techniques for identifying attacks and assessing their security. The aim is to assess and further analyze the need for enhancement of the attack identification approach for WSN's security posture to improve. This research is based on a systematic review, where the articles concerning the WSNs, IoT, Industrial IoT, Cybersecurity, attack identification, and assessment are identified, examined, and explained. The research question remains on WSNs and techniques for identifying attacks and assessing their security. To reinforce industrial safety for any event of cyber-attacks occurring. We conducted a detailed search across leading databases: IEEE Xplore, Elsevier ScienceDirect, and ACM Digital Library. To operationalize the search, we looked for various keywords related to Wireless Sensor Networks (WSN) and techniques for identifying attacks and assessing their security. Keywords used were (WSN OR security OR attacks OR identification OR assessment). Our initial search found many articles, of which 200 were selected for checking based on title and abstract relevancy. These selected papers were then passingly evaluated for eligibility for the study. We applied a series of inclusion/exclusion criteria. Articles were considered if they were if they were (1) published in the last five years, aligning with the emergence of new technologies for Industry 4.0, (2) written in English, and (3) focused on WSN security, attack identification, and IoT/IIoT security measures. Thus, irrelevant articles are excluded if they (1) were review articles without comparative data analysis, (2) did not directly address WSN security in the context of IoT or IIoT, or (3) lacked a focus on attack identification techniques and security assessments. For this selection, after applying inclusion/exclusion criteria we were left with a total of 60 articles that fulfilled the criteria and were included in the final study. Additionally, for the selected papers systematic review records are kept written which supports and shows why they were chosen and further used in data extraction and analysis.

A. Data Extraction and Analysis

The data extraction process was supervised based on the findings of 60 articles that met our inclusion criteria. To extract the data from the study articles and check the suitability of the data, the process of extracting data is accomplished in the full examination of each article. Key information extracted included study authors, year of publication, research themes, methods employed, technologies used, metrics evaluated, key findings, and identified gaps. To analyze the extracted data, we employed a mixed-methods approach that combined quantitative and qualitative analysis techniques. We conducted a statistical analysis of the year of publication data to identify trends over time, assessing the growing interest and research output in WSN security. For the qualitative component, we used thematic analysis to synthesize and interpret the findings from the selected articles. This involved coding the extracted data for recurring themes related to secure communication techniques, intrusion detection methods, and IoT/IIoT security challenges. The findings from our data analysis were interpreted within the broader context of WSN security's role in safeguarding IoT and IIoT ecosystems.

Below Table I presents a comprehensive summary of the studies included in the review, focusing on WSN security techniques and algorithms. The table categorizes the studies based on their year of publication, allowing for an examination of trends over time in research output related to WSN security. The distribution between years reveals a highlighted increase in publications from 2018 to 2021, with the highest number of publications recorded in 2021. This trend suggests a growing interest and emphasis on addressing security challenges in WSNs, particularly in the context of emerging technologies such as IoT and IIoT. By systematically organizing the data in this manner, our analysis aims to provide insights into the evolving landscape of WSN security research and highlight areas of focus within different periods.

TABLE I. SUMMARY OF THE STUDIES INCLUDED IN THE SYSTEMATIC REVIEW

Year of publication	Number of publications
2018	4
2019	10
2020	13
2021	19
2022	11
2023	4
Total	60

A systematic review found data corresponding to the key-extracted data. Further to assess the quality and validity of these data we took the articles to thematic analysis. By taking this into account, the article analysis we have papers that align with each constructed theme. This decreased the number of qualitative papers.

It appears that no papers were found that directly align with the approach of attack identification. We further conduct a methodological analysis to analyze the methods used across the papers. We have discovered the most frequently mentioned methods in the papers, by extracting and analyzing the research method from the systematic review written records. Based on the systematic review, research from the selected papers important findings and discussion will be provided in the following section

B. Findings and Discussion

WSN is considered a component of the communication infrastructure of Internet of Things (IoT) sensors, but Cybersecurity remains a challenge to maintain at the proper level. WSN composition includes nodes, routers, and a gateway. These sensor networks are used for monitoring and collecting data from diverse physical locations. The relationship or common point of IoT with Wireless Sensor Networks (WSN) refers to the distributed group of sensors in a geographical space for monitoring, and collecting data, and automatically passing them through the wireless network to the central location. The major highlight found on WSN's close relation to IoT and IIoT in all 60 selected papers, explicitly answers our first research question, that securing WSN will highly affect the IoT and IIoT overall Cybersecurity. As we have presented in the sections above, the articles papers were selected for research, further analysis, and the production of results in the categorization of the themes. Furthermore, in this section, we will present the findings, and discuss each theme using the point evidence explanation method and use these findings as a basis for our second part of the research where we perform the simulation experiment and aim to answer the second research question.

C. Theme 1: Techniques for Secure Communication in WSN

Paper [2] indicates the need to ensure sustainable network security and privacy protection in this evolving environment of the electricity Internet of Things (IoT). More precisely, [2] goes further into the challenges and vulnerabilities that exist in electricity IoT, stressing the importance of addressing these issues to provide efficient operation of modern energy systems. The finding of these vulnerabilities not only presents the existing security gap in electricity IoT but also underlines the potential risk of them being exploited by malicious actors, which would harm the power network. It uses a shared security key and random numbers for mutual authentication, ensuring secure and efficient operation against common cyber threats example man-in-the-middle attacks (MiTM). The protocol application consumes less network bandwidth, reduces complexity, and is specifically designed to meet the needs of smart grids, exhibiting improvement in encryption and decryption times compared to traditional algorithms like DES and RSA The Internet of Things (IoT) has brought innovative chances, but with them come risks and security threats, and the need for Cybersecurity in communication is necessary.

The study [4], is a comprehensive study of novel Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for Internet of Things (IoT) networks. Outlines various methodologies and mechanisms for attack detection and prevention in IoT networks It emphasizes advanced techniques like anomaly detection based on machine learning algorithms, signature-based detection for known threats, and hybrid systems that combine multiple approaches for enhanced accuracy. The following machine learning algorithms are used for intrusion detection and prevention in IoT networks: Random Forest (RF), Extreme Gradient Boosting (XGBoost), Parallel Deep Auto-Encoder (PDAE), K-Nearest Neighbors (KNN), Deep Neural Network (DNN), etc. The top two methodologies based on their effectiveness in intrusion detection and prevention within IoT networks are Distributed IDS Using Fog Computing and ML-IDS for IoT Network attack identification. These two methodologies demonstrate cutting-edge approaches in the field of IoT security, offering high levels of accuracy, efficiency, and applicability in real-world scenarios. The paper is related to the focus of this theme of secure communication techniques in WSN, as it highlights the importance of sustainable systems that can predict, detect, and neutralize potential threats, and attacks. An essential aspect of secure communication is trust, especially in infrastructures integrated with WSN and IoT.

The paper [5] discusses secure communication techniques through the lens of information trust models in WSN-assisted IoT, focusing on the utilization of Data Fusion Trust (DFT) models and their results in enhancing the security and reliability of data communication. The study focuses on the analysis of different levels of trust information, especially the importance of trustworthiness to provide solid and secure communication in these networks. The integration of WSN with IoT brings serious challenges in terms of security and trust. By understanding and implementing sustainable trust models, and a multi-level approach, it becomes clear that improved security of communication ensures that the exchanged data is not only efficient but also protected from potential threats. The detection of malicious nodes in WSN is vital for preserving the integrity and efficiency of communication.

In this study [5] empirical evaluation focused on malicious node detection within a WSN environment is provided. The research is based on experimental evaluation, providing methodology and results to show the effectiveness of certain detection mechanisms. It is very important to detect malicious nodes, which can damage the security and stability of the WSN, causing data breaches. Thoroughly the approaches of this study are deterministic and non-deterministic for DFT assurance. The deterministic approaches focus on securing the integrity and validity of data fusion processes through witness verification and voting mechanisms. These methods aim to tackle false data injection and message alteration attacks effectively. Non-deterministic approaches leverage probabilistic models and reputation systems to secure data aggregation against malicious activities, enhancing the trustworthiness of fusion results. At a time when the use of IoT devices is exponentially higher, providing secure communication is a challenge, especially knowing that their application in different industry sectors has occurred.

Paper [6] looks at the complexity of proving a security framework for IoT devices specifically using Physical Unclonable Functions (PUFs). The authors of the study notice with special emphasis and provide information about vulnerabilities that are often overlooked by traditional security methodologies when applied to IoT. Focusing on the low-cost approach, the study shed the light that security does not often have to have a high cost. The security of the proposed PUF-based schemes in next-generation IoT networks focuses on two main security protocols based on PUF implementation. These protocols aim to influence providing secure communications and authenticate devices within IoT networks. Rather, with the right strategies and understanding of the IoT environment, it is possible to achieve the most unbreakable security against attempts to compromise. The paper addresses the critical challenges for providing secure communication and presents the Metric-based RPL Trustworthiness Scheme (MRTS) for enhancing IoT security through trust-aware routing in the WSN [7]. The study continues in-depth on the complexities of routing protocols, focusing on the integration of the trust mechanism to increase the security of the data transmitted through the WSN. By making such integrations, the authors specify the importance of reliable evaluations to decide which path is more secure for data transmission. It highlights the evolution towards trust-based protocols that effectively manage the cluster-based structure of WSNs, combining trust-based routing with multipath logic for improved security and network performance. MRTS leverages trust, energy, and link quality metrics for routing decisions, aiming to isolate malicious nodes and ensure secure data transmission. Increasing security in wireless medical sensor network systems is significant, knowing the sensitivity of medical data and the threats, and attacks that constantly target them. [7] studies in detail the security aspect of three-factor authentication, which leads further toward tighter security for wireless medical sensor networks. Such mechanisms in WSN are necessary, more precisely in the field of medicine where the confidentiality and integrity component must be protected.

In [8] a comprehensive survey examines vulnerabilities related to Advanced Metering Infrastructure (AMI) within smart grids, provides information on potential attacks, and proposes countermeasures for the protection of these systems. The study recalls the urgent need to address communication security in the WSN domain. The study highlights the importance of data encryption, authentication mechanisms as prevention, and intrusion detection systems as key countermeasures to safeguard AMI systems against various cyber threats. Effectiveness is assessed based on resilience to cyber threats, enhancement of data confidentiality, integrity, and system availability.

Paper [9] handles ensuring secure communication in IoT infrastructure, which is a subset of WSN; and focuses on the development and analysis of the trust-aware routing protocol for IoT, with the aim that this protocol increases the level of security and reliability in data transmission between devices using WSN. The paper introduces the Metric-based RPL Trustworthiness Scheme (MRTS), to advance IoT security by avoiding malicious nodes and selecting the most trusted path for data routing. Results indicate improved packet delivery ratio, reduced energy consumption, stabilized node rank, and increased throughput, demonstrating MRTS's capability to secure routing in IoT networks against vulnerabilities and attacks, thereby ensuring reliable and efficient communication. MRTS uses trust evaluation for secure routing topology construction, effectively addressing vulnerabilities in the Routing Protocol for Low-Power and Lossy Networks (RPL) to attacks. It utilizes game theory concepts to formalize cooperation enforcement among nodes. This approach combines detailed network modeling, mathematical analysis of routing metrics, and game theory to address IoT security challenges.

Paper [10] sees an in-depth analysis of the clustering protocols of WSN, noticing their role in the advancement of network efficiency and long living; but the energy constraints in WSN, clustering, and data aggregation are highlighted as important techniques. It discusses varied protocols like LEACH and its variants, TEEN for reactive networks, and energy-efficient clustering protocols. LEACH significantly contributes to security in Wireless Sensor Networks (WSNs) by employing dynamic cluster head rotation, which enhances network resilience against node capture attacks and eavesdropping. Additionally, techniques range from LEACH and its variants, focusing on self-organizing and adaptive clustering, to TEEN and APTEEN, designed for time-sensitive data delivery. Amongst mathematical modeling, such as probability-based cluster head selection and energy-efficient routing algorithms, these protocols achieve a balance between energy conservation and effective data transmission, significantly impacting the performance and sustainability of wireless sensor networks. The key mathematical models and algorithms detailed in this study include the Bellman-Ford Algorithm, ERNT, and Isotonicity and Monotonicity Properties.

The focus [11] is on influencing lightweight and efficient security mechanisms to defend data integrity and authenticate nodes, crucial in the context of resource-constrained environments. Digital watermarking emerges as a core technique, embedding unique markers in sensory data to verify its authenticity and integrity. These techniques illustrate a strategic balance between enhancing security measures and managing the limited computational and energy resources inherent to WSNs.

Paper [12] provides a comprehensive overview of security concerns in UWSNs, detailing various security attacks and their countermeasures. It scales different layers of network architecture, offering insights into passive and active attacks, node capture, jamming, and DoS attacks, among others.

Ref. [13] defines a comprehensive classification of security attacks and corresponding security solutions across the different layers of IoT, including the perception, network, and application layers. Through all layers, a mix of symmetric and public key encryption, hash-function-based encryption, IP Security, and both intrusion prevention and detection mechanisms are illuminated as critical to defending IoT environments against a wide range of threats.

Ref. [14] examines the use of genetic algorithms (GAs) for optimizing the distribution of cluster heads within a wireless sensor network (WSN) to enhance connectivity and energy efficiency. The results demonstrate the effectiveness of GAs in optimizing WSN configurations, leading to more efficient and reliable network operations.

Ref. [15] a novel hybrid model for secure data transmission in Wireless Sensor Networks (WSNs) that integrates RSA encryption with the Efficient Data Collection and Dissemination (EDCD) algorithm to significantly reduce energy consumption. By selectively encrypting data based on the significance of changes, the model optimizes energy use, crucial for extending the operational lifespan of sensor nodes.

Ref. [16] enhance IoT network security by combining lightweight encryption protocols, specifically enhancing the Datagram Transport Layer Security (DTLS) protocol and incorporating an overhearing mechanism. The study exhibits using simulation the effectiveness of this solution in enhancing security while managing resource consumption challenges inherent to IoT environments.

Ref. [17] evaluates various communication protocols, primarily ZigBee, for their energy efficiency, routing topologies, and security challenges in IoT applications. The study highlights ZigBee's role in low-power, low-cost IoT solutions, addressing security vulnerabilities to active and passive attacks. Ref. [18] systematic literature review on trust-based security for Wireless Sensor Networks (WSNs), assessing designs, applications, protocols, and trust factors across 140 publications. The findings underscore the importance of designing efficient trust management systems to ensure the reliability and security of WSNs. Ref. [19] introduces a consensus-based secure and efficient compressive sensing (CSCS) model for wireless sensor networks (WSNs), designed to enhance network security and data transmission efficiency. Utilizing this approach, the performance evaluation of the CSCS model demonstrated improvements in energy utilization, correct node identification, and reduced misidentification of nodes compared to existing models. Ref. [20] suggests an adaptive security approach for WSNs using RSA algorithms, distinguishing between light and heavy RSA versions based on node power levels to optimize energy use and maintain security. This way selectively employs either a heavy or a light version of the RSA algorithm based on the residual power of the sensor nodes, optimizing for energy efficiency without compromising security. Ref. [21] a three-stage consensus-based security model for IoT networks, focusing on secure data sharing. It features an innovative approach that includes an initial setup for sensor thresholds, efficient data packet transmission, and secure routing to discard unsecured nodes. This model is valued based on energy consumption, malicious packet detection, and throughput, demonstrating superior performance over existing models. Ref. [22] a comprehensive analysis of security threats in WSNs and IoT, categorizing attacks into passive and active types, and detailing defense solutions such as encryption, anomaly detection, and multi-path routing. It emphasizes the importance of incorporating defense mechanisms like the geographic routing protocol to mitigate sinkhole and wormhole attacks. Ref. [23] addressing the critical aspect of securing these networks through effective key management protocols. The study underscores the importance of adapting key management strategies to the unique constraints and requirements of WSNs, such as limited computational resources, energy constraints, and the need for secure communication channels. Ref. [24] deep dive into a privacy-preserving technique utilizing multi-hop dynamic clustering and elliptic curve cryptosystem for Wireless Sensor Networks (WSN) in IoT environments. It introduces the Optimal Privacy-Multihop Dynamic Clustering Routing Protocol (OP-MDCRP) to enhance data privacy and energy-efficient routing. It also introduces a high data privacy method using the Elliptic Curve Integrated Encryption-Key Provisioning Method (ECIES-KPM), focusing on security against data-based attacks with minimal computational overhead.

Proposes a dynamic strategy to prevent node capture attacks by frequently updating authentication information among sensors and gateways. The scheme utilizes cryptographic methods to ensure secure exchanges, thus addressing potential security vulnerabilities in WSNs [25]. Ref. [26] discusses secure communication techniques within the context of Wireless Sensor Networks (WSNs), particularly focusing on a novel privacy-preserving approach utilizing multi-hop dynamic clustering and elliptic curve cryptography. This approach is designed to enhance both the privacy and energy efficiency of WSN communications.

D. Theme 2: Algorithms and methods for intrusion detection in WSN

Algorithms and methods for intrusion detection are key, particularly while devices are connected in a multi-service environment. Ref. [27] studies IoT by proposing a trust management framework utilizing the Probabilistic Neighbourhood Overlap (P-NO) for assessing and managing trust in Social Internet of Things (IoT) networks. The framework supports multi-service environments, enabling dynamic and static trust assessments to ensure reliable service provider selection. It employs a mix of direct and indirect opinions, utilizing a hybrid approach that balances the benefits of interaction-based and graph-based trust assessment methods. This model is designed to evaluate the trustworthiness of nodes within an IoT network by considering both direct and indirect interactions, leveraging data from social networks and IoT device behaviors. At the moment in the IoT infrastructure, the device evaluates and decides on the trustworthiness of its peers, thus creating a security layer that can identify the potential threat - the study presents. The challenge for intrusion detection in WSN remains the one caused by selective forwarding attacks in scale-free networks.

Ref. [28] explores this issue by introducing a security routing algorithm named MPSR (Multiple Paths Secure Routing), aimed at countering selective forwarding attacks in scale-free networks; the study contributes to the theme, recalling the critical need for the development of algorithms for securing networks against targeted forwarding attacks. This algorithm engages a multi-attribute decision-making model, incorporating node attributes like load, energy transmission efficiency, and packet loss rate, to improve network security and energy efficiency. Based on its decision-making model algorithm employs a multi-attribute decision-making model that uses these attributes to evaluate and select the optimal routing paths. Simulations demonstrate MPSR's effectiveness in avoiding malicious nodes and improving both the security and energy efficiency of network routing.

Ref. [29] studies the complexity of threats and attacks targeting sensors, smart devices, and applications; and presents a broad outline of the various threats and vulnerabilities that appear concerning IoT. The survey highlights the lack of adequate security mechanisms to control sensor access by installed apps, making smart devices vulnerable to these attacks. The paper contributes to the aligned theme, in the identification, and classification of threat-related sensors; to develop and improve intrusion detection algorithms dedicated to WSN. It provides a comprehensive overview of existing threats and outlines countermeasures against sensor-based threats on smart devices, emphasizing enhancements in sensor management, intrusion detection systems, data protection, and app security analysis.

Ref. [30] deep dive into the IIoT environment, the diversity of devices and the complexity of data exchange, the need for a sustainable security standard; comprehensive exploration of current standards, highlighting vulnerabilities, and potential threats, and proposing countermeasures as a fortification against attacks. The study systematically reviews various Cybersecurity standards for the Industrial IoT, emphasizing the integration of advanced technologies like AI, machine learning, blockchain, and 5G/6G networks to combat security threats. The review concerns the importance of developing thorough security measures including the use of machine learning for threat detection, the application of blockchain for decentralized security, and the integration of 5G networks to improve connectivity and resilience. Furthermore, it considers the development of tailored cybersecurity frameworks for IIoT environments, the implementation of intelligent DoS detection frameworks, and the enhancement of secure MQTT communication protocols. The increase in the use of IoT in different industry sectors has brought challenges, in data errors from the sensitiveness of sensors and environmental interference.

Ref. [31] represents the need for effective anomaly detection methods for IoT; the idea of the edge-based approach, the methodology used has given detection accuracy from 93% to 100%. The approach involves two phases: data clustering using the Gaussian Mixture Model (GMM) to separate normal from anomalous data and credibility calculation using fuzzy measures to evaluate the reliability of the data clusters. By clustering data based on statistical distributions and assessing cluster credibility through fuzzy measures, this method effectively distinguishes between normal and anomalous behaviors without requiring extensive training datasets.

Ref. [3] investigates cyber threats for Industrial IoT systems and sensors and presents a comprehensive model for Cybersecurity standards in the Industrial IoT sensors; the study provides an experimental assessment of attacks and vulnerabilities in Industrial IoT. It defines the model approach into four-phased starting with extensive penetration testing to identify vulnerabilities, it proceeds to filter and sort these findings based on severity. Recommendations for cybersecurity countermeasures are then developed, informed by the analysis of vulnerabilities and best practices. The model concludes with a cost-benefit analysis of these recommendations, which come in a final report that guides organizations in implementing the most effective security solutions and baseline.

Ref. [1] shows us the role of fuzzy set theory in identifying cyber-attacks in WSN; the study highlights the importance of algorithms and methods, to distinguish threats to WSN. It presents a method that leverages fuzzy and linguistic variables to process knowledge about potential attacks, aiming to enhance the reliability of security control in modern systems and networks.

The paper [32] investigates higher methodologies for detecting malicious nodes in WSN, focusing on combating false data injection (FDI) attacks; the study proposes correlation detection methods to find malicious activities in WSN nodes; Correlation as a method of detection works on the principle of finding patterns and connections between data points or events. Experimental results demonstrate enhanced recall and reduced false-positive and false-negative rates compared to traditional models, showcasing the effectiveness of this method in improving the security and reliability of WSNs. Ref. [33] presents a new approach related to the use of a full host-based attack graph to assess vulnerabilities and threats in WSN; it constructs a host-based attack graph model, utilizes splitting algorithms for weakly connected components, and assesses network security and key nodes using degree centrality and betweenness centrality; the study proposes focusing on host-based metrics gives us a better understanding and mitigation of threats. In [34] explores the possibilities of prediction related to spoofed

ACK packet attacks that target WSN nodes; the study proposes the prediction of Distributed Denial of Service (DDOS) attacks on WSN nodes, enabling taking proactive measures to protect the network with more advanced algorithms and methods. It emphasizes an experimental approach that involves various transmission behaviors to identify DDoS activities with high accuracy. The study emphasizes the importance of a 23-millisecond delay between transmissions to prevent overwhelming the network, showcasing the method's effectiveness in enhancing WSN security against DDoS attacks by accurately distinguishing malicious traffic patterns.

At [35] research presents a technique that detects face spoofing attacks by integrating Local Binary Patterns (LBP) using a colour-texture-based deep neural network technique. It integrates Local Binary Patterns (LBP) with convolutional neural network-based transfer learning models to analyze color spaces (RGB, HSV, YCrCb) for distinguishing between real and spoofed faces. This method demonstrates superior effectiveness over existing techniques, with extensive experiments conducted on the NUAA benchmark dataset showing high accuracy in identifying spoofing attempts.

In [36] analysis of the integration of Wireless Sensor Networks (WSN) within the Internet of Things (IoT) ecosystem. Furthermore, it addresses the challenges of securing WSN-IoT systems and proposes future directions for research, focusing on multi-hosted network transmission, low-power systems design, and enhancing security protocols. Ref. [37] introduces an innovative security system designed for WSNs, focusing on adaptive and intelligent alarm mechanisms to enhance security. This approach combines practical component selection with reliability, integrating automatic switchovers in power supply units for uninterrupted operation. The effectiveness is exhibited through comprehensive testing, aiming to offer an affordable and robust method to monitor and deter unauthorized access.

Ref. [38] examines the effectiveness of data mining techniques for detecting Denial of Service (DoS) attacks in WSNs. It examines several algorithms, including KNN, SVM, Logistic Regression, and ANN, for their ability to identify various DoS attacks such as Blackhole, Grayhole, Flooding, and TDMA. The study found ANN and Logistic Regression to be highly effective in detecting DoS attacks in WSNs, with ANN showing remarkable accuracy in real-time applications. In [39] surveys various countermeasures against Sybil attacks in IoT-based WSNs, emphasizing encryption, trust mechanisms, RSSI-based methods, and artificial intelligence. It critically evaluates each strategy's effectiveness, exhibiting encryption and RSSI as the most prevalent solutions, each constituting 29% of the approaches reviewed.

In [40] deep dive into a variety of algorithms and methods for intrusion detection in Wireless Sensor Networks (WSNs), presenting a broad spectrum of approaches designed to protect these networks from unauthorized access and malicious attacks. analysis reveals IDS techniques for WSNs and IoT with high detection rates of up to 99.87% and low false positive rates as minimal as 0.13%, showcasing their efficacy and specificity across various network types.

E. Theme 3: IoT and IIoT security concerning WSN

In [41] provides a deeper exploration of Cybersecurity standards for Industrial IoT; the study provides information on security and existing protocols used by IIoT systems, which includes WSN; furthermore, the study provides findings from the aspect of effective security measures that can be applied to protect against potential threats. In [42] provides a comprehensive exploration of current WSN security, highlighting their role in IoT and IIoT devices; this study presents the threats that succeed in targeting and notes some areas that need security improvement in WSNs in IoT and IIoT.

The paper [43] studies in detail the layers of security, privacy, and trust issues that each one faces, in connection with WSN; the study mentions the importance of an integral approach, recognizing vulnerabilities in a layer that can compromise the entire system. In [44] the paper presents the analysis of vulnerabilities related to IoT edge devices, mentioning risk assessment and countermeasures; edge devices serve as the first point of entry between the physical and digital parts, and spotting these vulnerabilities first, gives you an advantage in protection and a proactive approach to threats and attacks.

The paper [45] looks to analyze the existing literature which is more on the privacy requirements and security defense at the application layer of IoT systems. This research work is a comprehensive exploration of security obstacles in the IoT domain. The [46] presents an innovative approach to advance security in Industrial Internet of Things (IIoT) environments through a three-factor authentication mechanism. This approach integrates biometrics, smart card technology, and user passwords to provide a robust layer of security that is both lightweight and efficient. Through security analysis using the Real-or-Random model and verification with tools like ProVerif, the scheme exhibits strong resilience against common security threats, positioning it as a viable solution for secure communication within IIoT frameworks.

Ref. [47] it proposes a hash-based mechanism that aims to preserve privacy while ensuring lightweight and efficient authentication and key exchange. This approach includes impersonation and key-offset attacks, without imposing significant computational overhead on the network entities. In [48] outlines the approach that aims to address privacy and security challenges inherent in the IIoT by leveraging blockchain's decentralized and tamper-resistant properties to ensure secure, transparent, and reliable data exchange among sensors. By encapsulating data into blocks, the proposed blockchain mechanism provides a robust defense against common cybersecurity threats, including falsification attacks and unauthorized access, while simultaneously facilitating efficient and transparent verification processes.

The paper [49] scheme leverages blockchain technology to advance the security and trustworthiness of key management processes in dynamic wireless sensor networks (DWSNs). By constructing a stake blockchain on a hybrid sensor network and implementing secure cluster formation and node movement algorithms, BC-EKM replaces traditional base station functions with a decentralized trust mechanism. Ref. [50] deep dive into the integration of artificial and computational intelligence within IoT and WSNs, highlighting their potential to revolutionize these networks through enhanced decision-making, predictive analytics, and automation. It examines varied computational intelligence techniques such as neural networks, fuzzy systems, and machine learning algorithms, and their applications in improving IoT and WSN functionalities. The study lists machine learning algorithms including Neural Networks, Fuzzy Systems, CNN, SVM, KNN, PSO, GA, ACO, FFA, ANFIS, Random Forest, LSTM, DTMC, and SNN, showcasing their applications in IoT and WSN for tasks ranging from decision-making and classification to optimization and predictive analytics. In ref. [51] presents a comprehensive overview of low-power wireless technologies for smart healthcare applications, focusing on their standardization, frequency bands, data rates, energy efficiency, transmission range, and reliability. It inspects various protocols such as RFID, Bluetooth/BLE, ZigBee, TSCH, and Wi-Fi HaLow, outlining their typical applications in healthcare monitoring, data acquisition, and environmental sensing.

The paper [52] gives a comprehensive analysis of cybersecurity threats and countermeasures in the Industrial Internet of Things (IIoT), covering phishing, ransomware, protocol attacks, supply chain, and system attacks. It highlights the need for robust security mechanisms, including intrusion detection systems, encryption standards, and secure communication protocols. In [53] reviews IoT security trends, seeing on protocols like CoAP, MQTT, BLE, DDS, EnOcean, and SigFOX, which bolster secure communication through mechanisms like DTLS, TLS/SSL, GAP, and hardware security modules. While each protocol has its benefits, such as energy efficiency and reliable message distribution, they also face limitations like vulnerability to specific attacks and privacy concerns. Ref. [54] examines the junction of the Internet of Things (IoT) and robotics, termed the Internet of Robotic Things (IoT), focusing on the convergence of sensing, actuation, artificial intelligence, and IoT platforms. It delves into emerging IoRT technologies, including sensors and actuators, communication technologies, and data fusion methods.

Ref. [55] analysis of design accounts for building credible Industrial Control Systems (ICS) security testbeds. The findings suggest a framework for enhancing confidence, trustworthiness, and acceptance of ICS security testbeds through well-defined design and evaluation processes. Ref. [56] an analysis of cyber risk assessment frameworks, risk vectors, and risk ranking processes specifically for IoT systems, including the Internet of Medical Things (IoMT). It critically reviews various cybersecurity risk frameworks like NIST, OCTAVE, ISO, and TARA, detailing their applications, benefits, and limitations within the IoT domain. Emphasize the importance of adapting existing risk assessment frameworks to address the specific vulnerabilities and threats inherent to IoT technologies. Ref. [57] steps in the integration of IoT for crop monitoring, disease prevention, irrigation control, soil management, chemical control, and machinery management, highlighting the use of sensors, network protocols, and data processing technologies. The highlight on network protocols and data processing for IoT in agriculture reviews IoT solutions, devices, platforms, and their applications in agriculture without a focused examination of security measures for communication within WSNs. In [58] discusses the differences and similarities in security challenges faced by IoT and WSN. It highlights the unique requirements of each for secure operation, focusing on aspects like encryption, authentication, and intrusion detection.

The paper [59] it addresses security requirements like data confidentiality, integrity, freshness, and authentication, and explores defense mechanisms against common threats such as DoS attacks, eavesdropping, and spoofing. The study introduces several defense mechanisms against common attacks in IoT and WSN environments including mechanisms like Spread Spectrum and JAM are proposed for mitigating jamming attacks, while REWARD routing and Secure backpressure algorithms are suggested for defending against black-hole attacks. In [60] introduces a secure and efficient three-factor authentication protocol for IoT environments, focusing on sensing devices. It leverages Physical Unclonable Functions (PUFs) and honey list techniques to defend against various attacks, including ID/password pair guessing, brute-force, and device capture attacks. The protocol aims to enhance IoT security through a combination of user biometrics, passwords, and device-specific PUF responses.

V. Research Part II – Simulation Experiment

To further show the research results for the attack identification approach, a WSN simulation experiment with nodes has been performed. Our experimental simulation was carried out designed to replicate a typical WSN environment and evaluate the effectiveness of attack identification approaches. Conducted on a robust PC environment with an i5 8th Gen CPU, 16 GB RAM, and Ubuntu OS, we leveraged the Contiki operating system and utilized the Cooja network simulator and Wireshark for packet analysis. Contiki OS, renowned for its lightweight, efficient, and highly configurable nature, offers an ideal operating system for simulating the complex dynamics of Wireless Sensor Networks (WSN), particularly in IoT and IIoT contexts. The purpose of this simulation is to evaluate the effectiveness of the attack identification approach in WSN nodes. With this section of the paper, we want to contribute to WSN nodes in IoT networks, whose main challenge remains the identification and handling of attacks on these nodes. Perhaps and surely, it will not be the last simulation, but a starting point for advancing the approach of identifying these attacks in WSN nodes.

Methodology - initially, the simulation incorporated a realistic WSN topology with the following specific elements:

- Nodes: A total of 12 nodes (Sky mote) sensors were deployed with random distribution across a predefined area. Node 1 served as the main node or gateway, with the remaining 11 functioning as standard network nodes.
- Scenario I: Simulated normal network operation without attacks, providing a baseline for network behavior.

- Scenario II: Built upon Scenario I by introducing Node 13 as a malicious entity programmed with sinkhole attack code, and Node 14 equipped with intrusion detection capabilities.

Metrics used for evaluation:

- Network Traffic: Quantity and patterns of messages transmitted by the malicious Node 13 versus the normal behavior observed in the baseline scenario.
- Node Attractiveness: The success rate of Node 13 in diverting traffic away from the main Node 1, as measured by the number of connections and messages rerouted.
- Detection Efficiency: The capability of Node 14 to identify and isolate the malicious node, is evaluated by time to detection and the subsequent change in network traffic patterns.

Considering the limits of hardware resources, the number of sensor nodes has been set at 14 nodes in total. Now scenario I includes the simulation under normal network operation conditions, then further introduces the sensor Node 13 malicious one, and then observes the result. Scenario II also includes normal operation, malicious node, and introducing sensor Node 14 the attack identification approach, in networks with all other nodes.

Malicious sensor node 13 uses compiled code for sinkhole attacks on nodes in the network, always trying to become more attractive to be chosen by nodes and reducing the role of main node 1. Fig. 1 shows the simulated network topology and the spatial arrangement of nodes within the network environment. The figure illustrates the layout of sensor nodes in the network, with each node represented by a distinct symbol. The main node is denoted by a specific identifier, while the remaining nodes are positioned relative to it. The spatial distribution of nodes is crucial for understanding the network configuration and the potential impact of malicious nodes on communication patterns. This figure serves as a visual aid to complement the detailed description provided in the preceding sections, offering readers a clear understanding of the experimental setup and the positioning of nodes within the simulated environment.

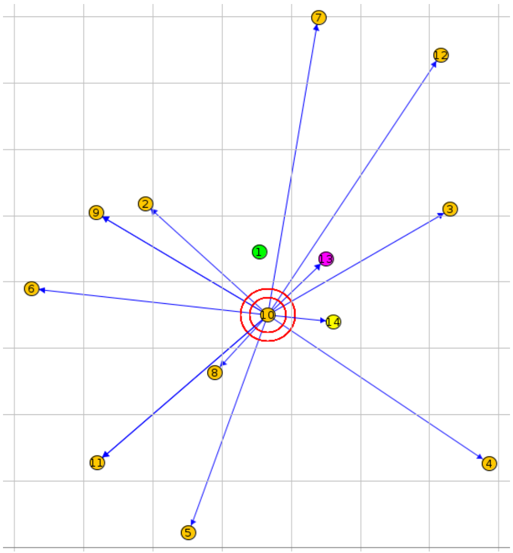

Fig. 1. Overview of nodes within the network on the simulator

Since the network with nodes is ready to conduct simulations for both scenarios, we will also adjust the configuration to collect log results from the simulations which will serve further in the next section results for analyzing and comparing among scenarios.

VI. Results

Based on the research objectives simulate a WSN node that would perform normal operation, introducing a malicious node as a sinkhole attack, and identification detection node of such malicious activities within the network. In this section a series of results will be given, to enforce the effectiveness of the attack identification approach.

Our simulation was done using the Contiki OS Cooja simulator, and we spotted the behavior of Wireless Sensor Network (WSN) nodes, referred to as "Motes" within this environment. Our focus was on the differencing of the patterns in radio messages and mote results during normal operation and the introduction of a malicious node in a sinkhole attack. The simulation provided pivotal insights, revealing that: Malicious Node 13 successfully altered network traffic, increasing its attractiveness to neighboring nodes, as indicated by the number of messages directed towards it, and diminishing the role of the main Node 1; The introduction of Node 14 showcased a marked improvement in the network's ability to identify and mitigate the sinkhole attack, as evidenced by changes in traffic routing and message patterns post-detection.

Throughout the normal operation, motes manifest a standard communication pattern, maintaining the network's integrity and ensuring consistent data transmission. However, from the introduction of a sinkhole attack by Mote 13, anomalies start to be noticed. Mote 13's interactivity with other motes deviated from the expected behavior, showing a higher message volume and increased communication with multiple motes. This high-volume activity is typical of sinkhole attacks, where the malicious node tries to divert network traffic toward itself, by promoting the favorable attracted node. It strives to divert traffic and have dominant communication, which notes the need for a detection mechanism of such threats in WSNs. Quantitative analysis summary of Scenario 1 baseline and sinkhole attack introduction:

- The malicious node, Mote 13, demonstrated a significant increase in broadcast and directed communications, totaling 275 and 98 messages respectively, indicating an aggressive attempt to reroute network traffic.
- Mote 13's interaction with specific nodes suggests a targeted approach to establish a sinkhole, with directed messages varying from 22 times to Mote 3 to 11 times each to Motes 2, 4, 6, 8, 9, 10, and 12.
- The absence of recorded messages from Mote 1, the root, during the sinkhole attack suggests an effective diversion of network traffic by Mote 13.

Scenario 2 sinkhole detection implementation:

- With the introduction of Node 14, the sinkhole detection node, there was a recorded total of 1178 messages sent by

Mote 13, pointing towards a high level of network activity and potential overcommunication as a bait tactic.

- The effectiveness of Node 14's detection mechanism can be inferred from the change in communication patterns post-detection, likely leading to a reduction in Mote 13’s traffic.

Fig. 2 displays the communication pattern of mote 13, designated as the attacker node in the sinkhole attack scenario. The figure visualizes the network traffic and communication interactions involving mote 13 during the simulation. Each bar in the chart represents a specific communication event involving mote 13, with the height of the bar indicating the intensity or frequency of communication during the simulation. This visualization offers a clear and concise representation of Mote 13's communication activities over time, providing valuable insights into the dynamics of the attack and its impact on network performance.

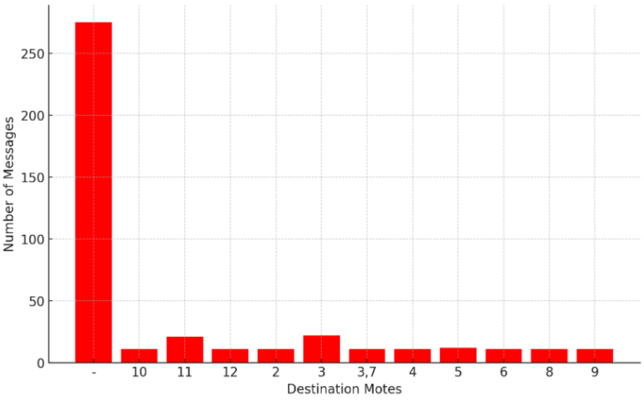

Fig. 2. Communication pattern of Mote 13 (attacker)

In the log results capturing the sinkhole attack, mote 1 the root, shows no communication. While we should expect the root node to have a presence actively in the network with other motes, its non-existence suggests that: sinkhole attacks have effectively rerouted traffic away from the root mote; otherwise, the attack intensity could have disrupted normal operations of the root mote, putting to its reduced or absent communication.

Based on the scenario results we provide a comparative analysis between scenarios 1 and 2:

- Comparing both scenarios suggests an enhancement in network resilience with the presence of the detection node, as evidenced by the change in Node 13’s communication behavior in the presence of Node 14.
- The metrics indicative of the sinkhole attack's impact and the subsequent response by the detection node offer a quantitative foundation to the study, bolstering the validity of the proposed attack identification approach.

Our simulation was done using the Contiki OS Cooja simulator, and we spotted the behavior of WSN nodes, referred to as "Motes", during the introduction of both a sinkhole attack and its following detection. This discussion leads us directly and unquestionably to the answer to our second research question, where clearly, we describe how the techniques for secure communication and algorithms for intrusion detection in WSN nodes illuminate the security issues. In this section above, we explained how mote 13 was identified as a sinkhole attacker, showing an untraditional communication pattern. The opposite of expectations, is its lack of direct communication, especially considering the nature of sinking attacks where the malicious node usually redirects or intercepts a significant number of messages, this was interesting. A reasonable explanation for this noticed behavior could be the efficiency of the sinkhole detection mechanism. More precisely, mote 14 might have detected and isolated mote 13, by challenging its malicious intent and protecting the network’s integrity.

Fig. 3 shows a histogram illustrating the distribution of all messages over time, offering insight into the communication pattern within the network. In this visualization, each bar represents a specific time interval, while the height corresponds to the frequency or volume of messages transmitted during that interval. A uniform distribution of bars suggests a stable and predictable communication pattern within the network, indicating normal operation. Conversely, irregularities or peaks in the histogram may signify deviations from the expected communication behavior, warranting further investigation for potential anomalies or security threats. This visualization provides a concise summary of message distribution dynamics over time, enabling stakeholders to assess the overall network performance and identify any aberrations that may require attention or remediation measures.

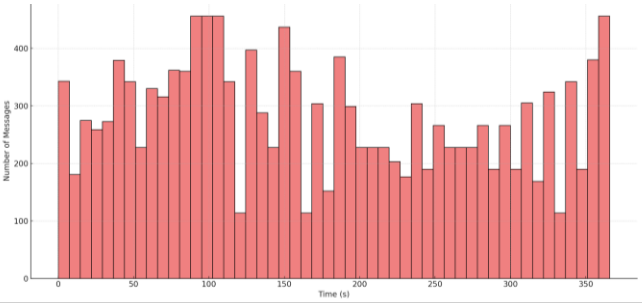

Fig. 3. Distribution of messages over time

The practical implications of our findings for WSN within IoT networks are highly relevant to the current cyber-security landscape. For instance, the enhanced detection capabilities observed in the simulation can inform the development of real-time security monitoring tools that actively scan for and mitigate sinkhole attacks, which are particularly false in distributed networks. For policymakers, our study supports the formulation of robust cybersecurity standards that encourage the integration of advanced detection technologies within WSNs.

VII. Conclusion

Our research conducted within the Contiki OS Cooja simulator drills down observations into the dynamics of Wireless Sensor Network (WSN) nodes during both normal operations and under the effect of a sinkhole attack. We have demonstrated that adaptive intrusion detection mechanisms can significantly enhance the security posture of WSNs, effectively mitigating the threats posed by such attacks.

These findings not only highlight the vulnerability of WSNs in IoT and IIoT environments to sophisticated cyber threats but also highlight the effectiveness of dynamic, real-time security strategies in addressing these challenges.

Curiously, at the time of the introduction of the sinkhole attack and its following detection, the node designated as the sinkhole attacker advertised unconventional communication patterns. This alteration, combined with our findings in the following scenario involving sinkhole detection, illuminates the potential efficacy of modern detection mechanisms in detecting and identifying threats, by protecting network integrity. The potential impact of our research extends beyond academic circles, offering a way for industry professionals, policymakers, and cybersecurity practitioners to navigate the complexities of securing IoT and IIoT ecosystems daily.

Although our research provides essential observations into WSN vulnerabilities and defenses, this is not without limitations. The performance of the algorithms evaluated may differ when subjected to the multifaceted challenges present in physical deployments. Variables such as signal interference, hardware heterogeneity, and diverse attack vectors in practical applications could influence the effectiveness of the attack detection and identification approaches observed in our study. Our review was focused on simulation environments, which while in a controlled environment, might not consider all real-world complexities. Additionally, in real-world deployments, environmental variables and hardware limitations could affect the performance of these algorithms. Our findings sound well with existing literature, which also mentions the keen nature of sinkhole attacks and the challenges in their detection. The noticed behavior of the malicious node in our simulation was like patterns identified in other studies. Additionally, the efficiency of detection observed in our study reflects the enhancements highlighted in contemporary research. Our study's results, compared with existing literature, insist on the persistent challenges in WSN security and offer empirical evidence of the potential benefits of adaptive detection mechanisms over traditional static defenses.

The insights from our study guide us in future research work. Although our simulation-based approach offers a foundation understanding, real-world testing can provide better and more practical results. A key direction for future research is the development of machine learning and artificial intelligence (AI) algorithms that adapt in real time to evolving attack patterns. Such adaptive algorithms would enhance the predictive capabilities of intrusion detection systems, allowing them to anticipate and mitigate attacks before they can exploit network vulnerabilities. The scope of future research will be expanded to encompass a thorough approach to enhancing the detection mechanisms for sensor network communications. This will not only include the improvement of strategies to counter sinkhole attacks but also extend to a rich palette of tools and methodologies aimed at addressing a broad spectrum of cyber threats. Furthermore, clearing the exchange among different types of attacks and designing a model that could provide enhanced defense strategies and resilience for WSN.

ACKNOWLEDGMENT

This research has been funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19680345).

REFERENCES

[1] V. A. Desnitsky, I. V. Kotenko, and I. B. Parashchuk, "Fuzzy Sets in Problems of Identification of Attacks on Wireless Sensor Networks," *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, pp. 290-293 2021, doi: 10.1109/elconrus51938.2021.9396712.

[2] R. Hou, G. Ren, C. Zhou, H. Yue, H. Liu, and J. Liu, "Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things," *Computer Communications*, vol. 158, pp. 64–72, May 2020, doi: 10.1016/j.comcom.2020.04.019.

[3] A. Buja, M. Apostolova, and A. Luma, "Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment," *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1-5, 2023, doi: 10.1109/meco58584.2023.10155100.

[4] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, "A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks," *Procedia Computer Science*, vol. 210, pp. 94–103, 2022, doi: 10.1016/j.procs.2022.10.124.

[5] I. Souissi, N. Ben Azzouna, and L. Ben Said, "A multi-level study of information trust models in WSN-assisted IoT," *Computer Networks*, vol. 151, pp. 12–30, Mar. 2019, doi: 10.1016/j.comnet.2019.01.010.

[6] N. A. Anagnostopoulos, S. Ahmad, T. Arul, D. Steinmetzer, M. Hollick, and S. Katzenbeisser, "Low-cost Security for Next-generation IoT Networks," *ACM Transactions on Internet Technology*, vol. 20, no. 3, pp. 1–31, Aug. 2020, doi: 10.1145/3406280.

[7] C. Konstantopoulos, B. Mamalis, and G. Pantziou, "Secure and trust-aware routing in wireless sensor networks," *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, pp. 312-317, 2018, doi: 10.1145/3291533.3291544.

[8] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Generation Computer Systems*, vol. 136, pp. 358–377, Nov. 2022, doi: 10.1016/j.future.2022.06.013.

[9] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," *Journal of Information Security and Applications*, vol. 52, p. 102467, Jun. 2020, doi: 10.1016/j.jisa.2020.102467.

[10] M. Raju and K. P. Lochanambal, "An Insight on Clustering Protocols in Wireless Sensor Networks," *Cybernetics and Information Technologies*, vol. 22, no. 2, pp. 66–85, Jun. 2022, doi: 10.2478/cait-2022-0017.

[11] T.-M. Hoang, V.-H. Bui, N.-L. Vu, and D.-H. Hoang, "A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks," *2020 International Conference on Information Networking (ICOIN)*, 2020, doi: 10.1109/icoin48656.2020.9016541.

[12] I. Ahmad *et al.*, "Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–15, Dec. 2021, doi: 10.1155/2021/1444024.

[13] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," *Sensors*, vol. 21, no. 11, p. 3654, May 2021, doi: 10.3390/s21113654.

[14] A. B. Alnajjar *et al.*, "Wireless Sensor Network Optimization Using Genetic Algorithm," *Journal of Robotics and Control (JRC)*, vol. 3, no. 6, pp. 827–835, Jan. 2023, doi: 10.18196/jrc.v3i6.16526.

[15] M. Mahmood Akawee, M. A. Meteab Al-Obaidi, H. M. Turki Al-Hilfi, S. I. Jassim, and T. Sutikno, "An efficient hybrid model for secure transmission of data by using efficient data collection and dissemination (EDCD) algorithm based WSN," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, p. 545, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp545-551.

[16] N. V. Tanh, N. Q. Tri, and M. M. Trung, “The solution to improve information security for IoT networks by combining lightweight encryption protocols,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 3, p. 1727, Sep. 2021, doi: 10.11591/ijeecs.v23.i3.pp1727-1735.

[17] S. W. Nourildean, M. D. Hassib, and Y. A. Mohammed, “Internet of things based wireless sensor network: a review,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, p. 246, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp246-261.

[18] R. Waseem Anwar, A. Zainal, and S. Iqbal, “Systematic literature review on designing trust-based security for WSNs,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 3, p. 1395, Jun. 2019, doi: 10.11591/ijeecs.v14.i3.pp1395-1404.

[19] N. S. Patil and A. Parveen, “Consensus-based secure and efficient compressive sensing in a wireless network sensors environment,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 1, p. 200, Apr. 2023, doi: 10.11591/ijeecs.v30.i1.pp200-207.

[20] M. S. Asaad and M. S. Croock, “Adaptive security approach for wireless sensor network using RSA algorithm,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, p. 361, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp361-368.

[21] R. H. Chamarajappa and G. C. Dyamanna, “A novel and distributed three phase consensus based secured data sharing in internet of things environment,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, p. 636, Aug. 2023, doi: 10.11591/ijeecs.v31.i2.pp636-646.

[22] S. Lata, S. Mehfuz, and S. Urooj, “Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies,” *IEEE Access*, vol. 9, pp. 161103–161128, 2021, doi: 10.1109/access.2021.3131367.

[23] N. Abd El-mawla, M. Badawy, and H. Arafat, “Security And Key Management Challenges Over Wsn (A Survey),” *International Journal of Computer Science & Engineering Survey*, vol. 10, no. 1, pp. 15–34, Feb. 2019, doi: 10.5121/ijcses.2019.10102.

[24] I. L. G and V. Kavitha, “Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 821–836, Jan. 2021, doi: 10.1007/s12083-020-01038-6.

[25] S.-K. Yang, Y.-M. Shiue, Z.-Y. Su, I.-H. Liu, and C.-G. Liu, “An Authentication Information Exchange Scheme in WSN for IoT Applications,” *IEEE Access*, vol. 8, pp. 9728–9738, 2020, doi: 10.1109/access.2020.2964815.

[26] R. Prodanović *et al*., “Wireless Sensor Network in Agriculture: Model of Cyber Security,” *Sensors*, vol. 20, no. 23, p. 6747, Nov. 2020, doi: 10.3390/s20236747.

[27] N. Narang and S. Kar, “A hybrid trust management framework for a multi-service social IoT network,” *Computer Communications*, vol. 171, pp. 61–79, Apr. 2021, doi: 10.1016/j.comcom.2021.02.015.

[28] R. Yin, F. Zhang, Y. Xu, L. Liu, and X. Li, “A security routing algorithm against selective forwarding attacks in scale-free networks,” *Procedia Computer Science*, vol. 174, pp. 543–548, 2020, doi: 10.1016/j.procs.2020.06.151.

[29] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, “A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021, doi: 10.1109/comst.2021.3064507.

[30] A. Buja, M. Apostolova, A. Luma, and Y. Januzaj, "Cyber Security standards for the Industrial Internet of Things (IIoT)," in *Proc. of the 1st Doctoral Colloquium on Sustainable Development*, pp. 1-6, 2022.

[31] W. M. Ismael, M. Gao, A. Zahary, Z. Yemeni, Y. Ibrahim, and A. Hawban, “Edge-based Anomaly Data Detection Approach for Wireless Sensor Network-based Internet of Things,” *2021 International Conference of Technology, Science and Administration (ICTSA)*, pp. 1-6, Mar. 2021, doi: 10.1109/ictsa52017.2021.9406548.

[32] Y. Lai *et al*., “Identifying malicious nodes in wireless sensor networks based on correlation detection,” *Computers & Security*, vol. 113, p. 102540, Feb. 2022, doi: 10.1016/j.cose.2021.102540.

[33] X. Wang, T. Zhou, and J. Zhu, “Network security assessment based on full host-based attack graph,” *Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies*, pp. 230-235, Dec. 2020, doi: 10.1145/3444370.3444577.

[34] M. A. Al-Naeem, “Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS,” *IEEE Access*, vol. 9, pp. 87070–87078, 2021, doi: 10.1109/access.2021.3089683.

[35] M. K. Rusia and D. K. Singh, “A Color-Texture-Based Deep Neural Network Technique to Detect Face Spoofing Attacks,” *Cybernetics and Information Technologies*, vol. 22, no. 3, pp. 127–145, Sep. 2022, doi: 10.2478/cait-2022-0032.

[36] F. F. Zijie, M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, “Wireless sensor networks in the internet of things: review, techniques, challenges, and future directions,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, p. 1190, Aug. 2023, doi: 10.11591/ijeecs.v31.i2.pp1190-1200.

[37] A. D. Salman, O. I. Khalaf, and G. M. Abdulsaheb, “An adaptive intelligent alarm system for wireless sensor network,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, p. 142, Jul. 2019, doi: 10.11591/ijeecs.v15.i1.pp142-147.

[38] M. Alauddin Rezvi, S. Moontaha, K. Akter Trisha, S. Tasnim Cynthia, and S. Ripon, “Data mining approach to analyzing intrusion detection of wireless sensor network,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, p. 516, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp516-523.

[39] A. Arshad, Z. Mohd Hanapi, S. Subramaniam, and R. Latip, “A survey of Sybil attack countermeasures in IoT-based wireless sensor networks,” *PeerJ Computer Science*, vol. 7, p. e673, Sep. 2021, doi: 10.7717/peerj-cs.673.

[40] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, “Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges,” *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/access.2019.2962829.

[41] A. Buja, M. Apostolova, A. Luma, and Y. Januzaj, “Cyber Security Standards for the Industrial Internet of Things (IIoT)– A Systematic Review,” *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-6, Jun. 2022, doi: 10.1109/hora55278.2022.9799870.

[42] Z. Huanan, X. Suping, and W. Jiannan, “Security and application of wireless sensor network,” *Procedia Computer Science*, vol. 183, pp. 486–492, 2021, doi: 10.1016/j.procs.2021.02.088.

[43] A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” *Future Generation Computer Systems*, vol. 108, pp. 909–920, Jul. 2020, doi: 10.1016/j.future.2018.04.027.

[44] G. George and S. M. Thampi, “Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things,” *Pervasive and Mobile Computing*, vol. 59, p. 101068, Oct. 2019, doi: 10.1016/j.pmcj.2019.101068.

[45] K. S. Sudha and N. Jeyanthi, “A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT),” *Cybernetics and Information Technologies*, vol. 21, no. 3, pp. 50–72, Sep. 2021, doi: 10.2478/cait-2021-0029.

[46] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M. A. Doostari, “LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT,” *Wireless Networks*, vol. 27, no. 2, pp. 1389–1412, Jan. 2021, doi: 10.1007/s11276-020-02523-9.

[47] S. Paliwal, “Hash-Based Conditional Privacy Preserving Authentication and Key Exchange Protocol Suitable for Industrial Internet of Things,” *IEEE Access*, vol. 7, pp. 136073–136093, 2019, doi: 10.1109/access.2019.2941701.

[48] G. Puthilibai, T. Benil, S. Chitradevi, V. Devatarika, D. R. Ashwin Kumar, and U. Padma, “Securing IIoT sensors communication using blockchain technology,” *2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, pp. 1-4, Dec. 2022, doi: 10.1109/icpects56089.2022.10047053.

[49] Y. Tian, Z. Wang, J. Xiong, and J. Ma, “A Blockchain-Based Secure Key Management Scheme With Trustworthiness in DWSNs,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, Sep. 2020, doi: 10.1109/tii.2020.2965975.

[50] G. Persada Nurani Hakim, D. Septiyana, and I. Suwarno, “Survey Paper Artificial and Computational Intelligence in the Internet of Things and Wireless Sensor Network,” *Journal of Robotics and*

Control (JRC), vol. 3, no. 4, pp. 439–454, Jul. 2022, doi: 10.18196/jrc.v3i4.15539.

[51] G. Gardašević, K. Katzis, D. Bajić, and L. Berbakov, "Emerging Wireless Sensor Networks and Internet of Things Technologies—Foundations of Smart Healthcare," *Sensors*, vol. 20, no. 13, p. 3619, Jun. 2020, doi: 10.3390/s20133619.

[52] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, Mar. 2021, doi: 10.3390/iot2010009.

[53] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: a survey," *SN Applied Sciences*, vol. 3, no. 1, Jan. 2021, doi: 10.1007/s42452-021-04156-9.

[54] O. Vermesan *et al*., "Internet of Robotic Things – Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence and IoT Platforms," *Cognitive Hyperconnected Digital Transformation*, pp. 97–155, Sep. 2022, doi: 10.1201/9781003337584-4.

[55] U. P. D. Ani, J. M. Watson, B. Green, B. Craggs, and J. R. C. Nurse, "Design Considerations for Building Credible Security Testbeds: Perspectives from Industrial Control System Use Cases," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 71–119, Nov. 2020, doi: 10.1080/23742917.2020.1843822.

[56] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP Journal on Information Security*, vol. 2020, no. 1, May 2020, doi: 10.1186/s13635-020-00111-0.

[57] E. Navarro, N. Costa, and A. Pereira, "A Systematic Review of IoT Solutions for Smart Farming," *Sensors*, vol. 20, no. 15, p. 4231, Jul. 2020, doi: 10.3390/s20154231.

[58] V. Choudhary, A. Srivastava, A. Kumar, and S. Taruna, "Comparative Analysis of Security Issues and Trends in IoT and WSN," *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, vol. 14, no. 2, pp. 216–222, Jun. 2022, doi: 10.18090/samriddhi.v14i02.16.

[59] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues," *Electronics*, vol. 10, no. 19, p. 2365, Sep. 2021, doi: 10.3390/electronics10192365.

[60] J. Lee *et al*., "PUFTAP-IoT: PUF-Based Three-Factor Authentication Protocol in IoT Environment Focused on Sensing Devices," *Sensors*, vol. 22, no. 18, p. 7075, Sep. 2022, doi: 10.3390/s22187075.