Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Hydroponic Shield: Safeguarding Farming Systems with Interleaved Honeypot-Framing and MAC Security

Vaira Muthu K[1], Dr. Krishnakumar A[2]
[1]*Research Scholar, Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India.*
Assistant Professor, Department of Computer Science, Kamalam College of Arts & Science, Anthiyur, Tamil Nadu, India
vairamuthukaruppusamy@gmail.com,- ORCID: 0000-0009-29556682
[2] *Research Supervisor, Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India.*
Assistant Professor, Department of Computer Science, Kamalam College of Arts & Science, Anthiyur, Tamil Nadu, India.
krishna2c@gmail.com,- ORCID: 0000-0003-2290-6957

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

Introduction: Hydroponic farming relies heavily on Wireless Sensor Networks (WSNs) for monitoring and automation, making secure communication protocols essential. The Hydroponic Medium Access Control (HMAC) protocol manages data frame exchanges in such environments. However, conventional MAC-layer security solutions remain susceptible to sophisticated attacks, posing risks to data integrity and network stability. Addressing these vulnerabilities is critical to ensure reliable and secure operations in hydroponic farming systems.

Objectives: The primary objective of this research is to enhance the security and reliability of HMAC protocols in hydroponic farming by introducing a reactive intrusion detection and prevention framework. The goal is to safeguard data transmissions against channel-based attacks through advanced, node-level security mechanisms while maintaining efficient network performance.

Methods: To achieve the stated objectives, we propose a novel Honeypot-Framing Model for HMAC protocol (HFM-HMAC). This model integrates distributed honeypot engines within sensor nodes, enabling proactive detection and mitigation of intrusion attempts. A key innovation is the use of Wireless Interleaved Honeypot Frames (WIHFs), supported by a secure hash-based random frame-interleaving technique. These elements allow dynamic conversion of Interleaved Honeypot Frames (IHFs) into legitimate sequences, effectively deceiving and isolating potential attackers. Furthermore, neighbor-based intrusion alert systems are implemented to facilitate cooperative defense mechanisms.

Results: Extensive simulations demonstrate the effectiveness of HFM-HMAC in securing hydroponic WSN environments. Compared to existing security-enhanced MAC protocols such as WIHFM, SZ-MAC, and BASR, the proposed HFM-HMAC model achieves a performance improvement ranging from 20% to 25%. Key metrics evaluated include attack mitigation rate, packet delivery ratio, latency, and energy consumption, all of which show significant enhancement under the HFM-HMAC protocol.

Conclusions: The HFM-HMAC framework introduces a robust wireless honeypot methodology tailored for the unique requirements of hydroponic farming communication systems. By leveraging node-centric honeypot mechanisms and secure frame-interleaving, the proposed approach effectively counters open-channel attacks and enhances overall MAC-layer resilience. The simulation results validate the

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

practical potential of HFM-HMAC as a superior security model, paving the way for more secure and intelligent agricultural networks.

Keywords - Honeypot Security, Hydroponic Farming Systems, MAC Protocol, Wireless Sensor Networks (WSNs), Intrusion Detection.

INTRODUCTION

Hydroponic farming represents a revolutionary agricultural method that involves growing plants without soil, using nutrient-rich water solutions instead [1]. This technique offers numerous benefits, including higher crop yields, reduced water consumption, and greater control over environmental conditions, Fig. 1 depicit the basic hydroponic Farming. As hydroponic farming gains popularity worldwide, the integration of advanced technologies like WSNs becomes crucial for efficient monitoring and management of various farming parameters. The Hydroponic Medium Access Control (HMAC) protocol plays a pivotal role in facilitating communication and data management within hydroponic farming systems. By overseeing the management of data frames, HMAC ensures the seamless transmission of information among sensor nodes deployed throughout the hydroponic environment [2,3]. However, the reliance on wireless communication exposes the system to potential security threats, necessitating the implementation of robust security measures.

While existing MAC policies offer some degree of protection, they often fall short in defending against sophisticated attacks targeting hydroponic farming systems [3]. This underscores the urgent need for enhanced security protocols tailored specifically to the unique challenges of hydroponic environments. To address this need, the Honeypot-Framing Model for Hydroponic Medium Access Control (HFM-HMAC) is proposed.HFM-HMAC introduces a novel security approach by leveraging distributed honeypot-based mechanisms within sensor nodes [1-4]. Through the strategic deployment of Wireless Interleaved Honeypot Frames (WIHFs), secure hash-based random frame-interleaving, and node-centric honeypot engines, HFM-HMAC optimizes WSN channels to proactively counter various attackers. Unlike traditional MAC policies, HFM-HMAC converts Interleaved Honeypot Frames (IHFs) into legitimate sequences, thereby enhancing security against channel attackers effectively [5,6].

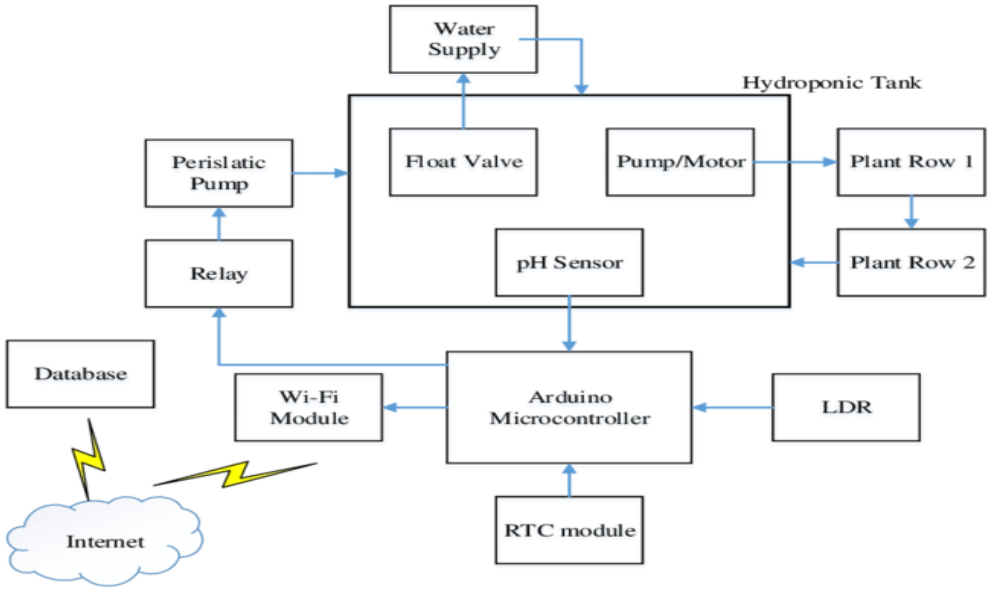

Figure 1. Basic Hydroponic Farming.

The implementation of HFM-HMAC ensures robust security standards and facilitates neighbor-based intrusion alerts, thereby safeguarding MAC frames in hydroponic farming environments. Moreover, HFM-HMAC's wireless honeypot methodology presents an innovative approach to countering open-channel attacks, providing a proactive defense mechanism against potential threats [7-9].

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In this paper, an exploration into the specifics of hydroponic farming and the role of MAC protocols in ensuring efficient communication within such environments is conducted. The critical need for enhanced security measures in hydroponic farming systems is discussed, along with an outline of the shortcomings of existing MAC policies in addressing these challenges. Furthermore, a detailed overview of the HFM-HMAC framework is provided, highlighting its key components and advantages over traditional security approaches. Finally, simulation results demonstrating the superiority of HFM-HMAC over existing techniques are presented, underscoring its potential to revolutionize security in hydroponic farming environments.

According to the outlined contributions, the proposed article has been structured into Sections 2–4. In this manuscript, Section 2 conducts an in-depth analysis of related techniques. Section 3 elucidates the distinctive features of the proposed HFM-HMAC framework and provides technical insights into the newly devised IHF solutions. Section 4 elaborates on and substantiates the contributions of the proposed HFM-HMAC through experimental results and performance comparisons. Finally, Section 5 encapsulates the overall contributions of the study and outlines the future scope of this innovative research article.

RELATED WORKS

WSNs have emerged as a pivotal area of research, particularly concerning their information security, which remains a hot topic. Palmieri & Campoverde [10] delve into the complexities of dynamic key management, combining an asymmetrical public key system with a threshold key scheme. They emphasize the significance of the second-level cluster-to-node authentication matrix. Similarly, Panahi, U & Bayılmış [11] advocate for an Enhanced Group Key Management Scheme tailored for Cluster-based WSNs, highlighting the hierarchical cluster structure's crucial role in designing effective key management and distribution strategies.

Understanding existing security solutions against various wireless channel attacks is foundational for developing future frameworks. Shrivastava [12] dissect infrastructure and data security models for unattended WSN environments, shedding light on vulnerabilities such as data modifications, false data generation, removals, and disclosures. However, they critique the lack of a versatile attacker detection system in their model, which primarily focuses on channel attainment over fundamental security benefits. Conversely, Al Mamun et al. [13] expound on the security dividends inherent in WSNs, ranging from location-sensitive security principles to distributed key management schemes. Their work culminates in the development of a WSN security model predicated on random location-based key selection, fortifying wireless MAC content.

Numerous endeavors aim to reconcile efficiency and security within WSNs. Sela Saldinger et al. [4] proffer a methodological approach to augment energy-efficient key management, premised on dynamic cluster head selection and message routing optimization. Meanwhile, Mamatha & Kavitha [15] pioneer an encryption-based routing technique, which encrypts both image and data streams for heightened efficiency. Simultaneously, Nikolov et al. [16] devise a method to test diverse face detection and identification algorithms, bolstering the security and reliability of online transactions.

Furthermore, concerted efforts are dedicated to mitigating specific security threats such as fabrication attacks, report interruption attacks, and node compromise attacks. However, these countermeasures often necessitate novel attacker-handling frameworks to achieve optimal efficacy. Additionally, the burgeoning industrial interest in the development of current WSN models cannot be overstated. Notable proposals like the Internet of Things (IoT) assisted flying ad hoc networks and energy-optimized routing strategies endeavor to surmount obstacles entrenched within energy-efficient routing protocols.

The below table 1 depicts the other related works [10-27].

Table 1. Related Works on Hydroponics and other WSN works

Title, Author and Year	Proposed Work	Findings	Limitations	Tools used	Future Research

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Automatic robotic system design and development for vertical hydroponic farming using IoT and big data analysis, Shrivastava et al., 2023	WSNs provide an easy and inexpensive way to monitor and control equipment.	WSN monitor agriculture affordably, CPS enhance precision farming, boosting crop productivity.	Complex Robotic algorithms to be implemented in a chip may cost high	Matlab	Investigate IoT, cloud tech fusion with WSN, CPS for better precision agriculture.
Predicting the intention and adoption of hydroponic farming among Chinese urbanites, Al Mamun et al., 2023	CEA uses complex math models for diverse design, control, higher automation .	Hydroponic techniques overviewed, pros/cons highlighted. Optimal plant growth methodologies discussed. ML prediction models proposed.	Integrating smart farming into CEA. Minimizing energy inputs. Enhancing productivity. Improving crop quality.	Matlab	Overcoming challenges. Integrating smart farming in CEA. Minimizing energy inputs. Enhancing productivity. Improving crop quality.
Hydroponic agriculture and microbial safety of vegetables: promises, challenges, and solutions, Sela Saldinger et al., 2023	Wireless sensor networks play a crucial role in advancing agriculture by transmitting data to the cloud and controlling variables such temperature and light.	Greenhouse findings represent an efficient agricultural technology, overseeing and managing factors such as temperature and light.	In hydroponic data will be processed and stored in the cloud. Therefore the chances of security breaches are also high. Need updates in security on time	NS 3	Future research may delve into exploring and optimizing WSN systems to advance agricultural development further.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine learning based crop growth management in greenhouse environment using hydroponics farming technique, Mamatha, & Kavitha, 2023	Cost-effective sensors enable farmers to monitor and optimize crop growth by efficiently managing resources in real-time.	The system integrates data from diverse sensors and delivers context-specific responses using fuzzy logic within a multi-agent setting.	Specific crop focus - Limited details on scalability and maintenance hurdles.	Matlab	To improve the adaptability and cost-effectiveness of automatic crop irrigation systems by incorporating machine learning techniques.
Design of a Small-Scale Hydroponic System for Indoor Farming of Leafy Vegetables, Nikolov et al., 2023	The suggested system can improve the growth of lettuce and bok choy plants, particularly in terms of leaf size.	Hydroponic agriculture is proposed as a remedy for limited agricultural land, with a monitoring and control system utilizing IoT and fuzzy logic for precision farming in hydroponics.	The emphasis lies on leaf size growth, which may not necessarily indicate overall plant health or encompass other growth parameters.	Matlab	Extending the system to oversee and regulate different plant varieties within hydroponic agriculture.
Environmental and health values, beliefs, norms and compatibility on intention to adopt hydroponic farming among unemployed youth, Gao et al., 2024	Automation of the hydroponic system amends the efficiency and reduces manual work.	Advancements in agriculture have proven beneficial for cultivators. Hydroponics is a technological advancement that minimizes space and water consumption.	Consumption of water and mineral solutions is a highly needed in hydroponics. Right mixture of solution to be identified based on the product.	NS2	Future research can focus on enhancing automation, incorporating IoT technology for remote monitoring and control.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A meta-analysis: Food production and vegetable crop yields of hydroponics, Goh et al., 2023	Sensors regularly measure pH levels of hydroponic supports and transmit data to a database.	The system alerts farmers about necessary corrective actions to prevent excessive acid and nutrient solution usage.	New rules integration in algorithms for autonomous irrigation controllers requires verification.	Java, PHP, HTML5, MySQL Server database.	Authors propose focusing on refining definitions of water quality parameters and integrating new rules for autonomous irrigation.
The role of plant growth-promoting microorganisms (PGPMs) and their feasibility in hydroponics and vertical farming, Dhawi, 2023	The proposed system is highly scalable and secure.	Introducing a smart climate and watering system controlled through an Android app, employing various sensors for live data collection, and integrating intelligent fuzzy logic for decision-making.	The effectiveness of the technologies enhances water resource utilization and ensures constant climate monitoring for the eight plants in this study.	Raspberry -Pi, Android applicatio n, Forecast API, MATLAB	Using genetic algorithms to improve neural networks for more accurate recommendations and predictions in the smart agricultural system.
Comparative analysis of IoT-based controlled environment and uncontrolled environment plant growth monitoring system for hydroponic indoor vertical farm, Kaur et al., 2023.	Automatio n of the hydroponic system improves the efficiency and reduces manual work.	Organic farming addresses cultivation challenges; agricultural advances are beneficial; hydroponics innovates plant growth without soil.	Vertical farming expenses are high initially.	Matlab	Automating hydroponic systems with IoT for remote control, reducing manual labor, enhancing efficiency.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Smart Greenhouse Technology for Hydroponic Farming: Is it Viable and Profitable Business?.Trisnasari & Saridewi, 2023.	Downstream water needs and penalties greatly impact reliability trade-offs in Montana's water system.	Study used linear programming and simulation to optimize crop combinations, water allocation, highlighting downstream water's impact on trade-offs.	Business tactics for hydroponic farming is to be identified based on the crop and geolocations.	Matlab	Develop advanced models for simulating multicrop water systems, emphasizing realism and broader management strategy evaluation.
Analysis of Economic Opportunities For Farming With Hydroponic Systems In Makassar City. Hikmah & Susanti, 2023.	Sensors link to Arduino Uno, Wi-Fi module ESP8266, and Raspberry Pi 2 Model B as webserver, employing IoT concept.	Study's system enables users to oversee and manage NFT hydroponic farming via web interface, enhancing effectiveness and efficiency.	Challenges: Human control reliance, manual nutrient monitoring, unaddressed technical failures, absent sustainability/scalability discussions.	NS2	Enhance system with camera for plant growth monitoring, pH regulator for water acidity control, and nutrient regulator for water nutrient concentration control.
Sustainable atmospheric water generator for hydroponic farming. Venu & Muralimohan, 2023.	Hydroponics agriculture production system gives promising yield round the year.	Hydroponics yields year-round, speeds vegetable/fruit growth; home-based tomato system includes growth/nutrient sensors.	Home-based tomato hydroponics study lacks comparisons, scalability, economic assessment.	NS2	Extend hydroponics to more plants, integrate AI for prediction, add sensors for monitoring.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Design and Implementation of an Automated Indoor Hydroponic Farming System Based on the Internet of Things. Niswar, 2023.	A smart farm can be made fully automated, log multiple sources of data and capable of wireless control.	pH level maintenance crucial in hydroponics; soft computing, fuzzy logic for automatic adjustments; pH affects plant photosynthesis.	Manual pH control may affect plant growth; DWC lacks automatic pH level maintenance.	Lab view, Raspberry Pi, Wi-Fi, Bluetooth	Enhance nutrient solution control algorithms/systems, investigate real-time pH monitoring/adjustment tech, study pH requirements for diverse plants.
Implementation of smart farming based solar cell system in hydroponic in the agricultural area of blitar village. Falah et al., 2023.	The system monitors water quality and greenhouse temperature and humidity.	iPONICS: Low-cost hydroponics for hobbyists, featuring wireless sensor network; smart farming noted as tech-intensive and capital-driven.	Sensor errors (drift, outliers) observed, occasional GPRS transmission failures noted, with reliability analysis based on 1000 hours of SCU and ESN operation, employing Poisson and binomial distributions for modeling, indicating system reliability at low sampling rates.	Arduino Mega 2560, Xbee shield, RTC shield, Atlas Scientific EZO circuits, GSM shield	Additional reliability analysis involves stress testing the system by inducing errors, while data analytics focuses on predicting nutrient values using original concentrations and water quality sensor readings.
A Smart Hydroponic Farming System Using Machine Learning, Kondaka et al., 2023.	The developed predictive controller makes use of soil moisture data at different depths.	Predictive controller reduces water, energy costs, maintains crop production; emphasizes need for accounting for nonlinear water dynamics in soil moisture-based irrigation control systems.	Lack of literature on addressed topic, stresses need to consider real water dynamics in soil for irrigation control, and notes reliance on traditional approaches by farmers/technicians.	NS2	Not Mentioned
The Effect of Marketing Mix on Repurchase Intention of Hydroponic Farm	The proposed methodology is embedded	The decision support system enhances irrigation	Geographic focus, limited generalizability to other agricultural settings, absence of	NS2	Extend methodology to other crops, integrate system with weather forecast for

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Vegetable Products. Rasyid et al., 2023.	the network gateway making the system a truly smart and autonomous wireless decision support system.	management, maximizing crop yield and water efficiency while reducing water waste, demonstrated in Italy vineyard trials.	comparisons with diverse crops or farming systems.		better irrigation scheduling.

Despite commendable strides, extant techniques are not without limitations. Node-centric intrusion detection systems, insufficient MAC confidentiality, and static connectivity models underscore the pressing need for innovation within WSN security paradigms. Thus, the proposed HFM-HMAC promises to redress these shortcomings with novel technical advancements. Section 3 delves deeper into the pivotal features and mathematical underpinnings of HFM-HMAC.

In essence, the discourse surrounding WSN security encapsulates a rich tapestry of research, innovation, and pragmatic solutions. Each contribution builds upon its predecessors, striving to fortify the integrity, confidentiality, and resilience of WSNs in an ever-evolving digital landscape.

PROPOSED HKM-HMAC FRAMEWORK

Channel-aware security principles and medium protection in WSNs have become pivotal in ensuring secure data communication. With WSNs comprising numerous sensor nodes and independent links for each channel, wireless sessions originating from these nodes are inherently vulnerable to suspicious activities and potential attacks. Therefore, safeguarding the wireless medium is imperative, necessitating the implementation of secure Medium Access Control (MAC) policies, secure link establishment mechanisms, and secure data transmission protocols.

To address the security requirements of the wireless medium, various cryptographic techniques and Distributed Intrusion Detection Systems (DIDS) procedures can be employed. As depicted in Fig. 1, proposed security features include novel interleaved honeypot frames, node-centric distributed honeypot engines, and measures for data integrity, confidentiality, authentication, and DIDS procedures. These channel-aware secure transmissions aim to fortify each frame before it traverses routing layer protocols.

MAC frames typically encompass essential elements such as MAC header fields encapsulated with frame control fields, session identifiers, source and destination MAC addresses, quality parameters, variable data heaps, frame protection bits, among others. However, open wireless MAC protocols remain susceptible to diverse channel attacks including jamming, false data insertion, identity theft, timing disturbances, and passive channel monitoring activities. Thus, comprehensive security measures are essential to mitigate these threats effectively.

The security features of the HFM-HMAC Framework is proposed below in Fig. 2. In the secure medium, counterattacking or protection schemes are deployed to mitigate unique attack patterns effectively. Wireless channels typically establish a secure MAC model by employing various cryptography techniques. These techniques include public key models, private key models, signature validation models, and other integrity-checking mechanisms. However, attackers may circumvent standard cryptography techniques by efficiently extracting the contents of MAC frames.

To address this challenge, the deployment of a novel MAC-framing solution offers unforeseen protection against channel attackers. This innovative approach enhances the security of MAC frames, providing a robust defense against potential threats in wireless communication channels.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

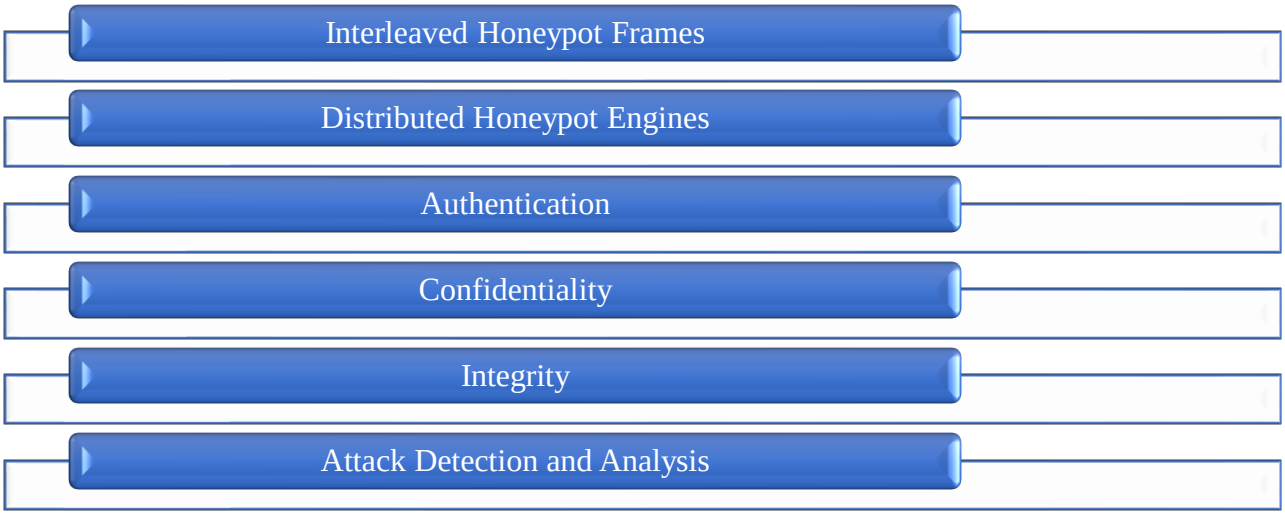

Figure 2. Proposed HFM-HMAC Framework

Therefore, the proposed model creates randomly generated IHFs to safeguard the streams of WSN frames. Building upon this concept, the subsequent sections detail the design of the network model, attacker model, suspicious event model, and the proposed channel-aware security principles.

WSN Model

In the assumed model of WSN, the quantity of sensor nodes is denoted as $'l'$, and the geographical area of the network is represented as $'a\ x\ b'$. The sensor nodes are responsible for discovering their neighbors and transmitting data to other nodes using wireless MAC protocol (IEEE 802.11) functions, as depicted in Equation (1).

$$Set_N = \begin{Bmatrix} 1 - active_N, Change_{time} \geq 1 \\ idle_N, Change_{time} < 1 \end{Bmatrix} \quad Eq.1$$

Appropriate basic channel model for WSN is detailed in Eq. 1. Set_N denotes set of nodes. $active_N$ represents active node participants of WSN and $idle_N$ signifies idle set of nodes. The $Change_{time}$ denotes changing time interval of a node that takes to change from active to idle state or idle to active states.

The proposed system introduces the On Demand Acyclic Connectivity model (ODAC) to facilitate the establishment of logical links between active sensor nodes. The ODAC model incorporates energy-sensitive connection establishment rules and association policies among the sensor nodes within an active channel.

Utilizing ODAC connectivity dynamics, logical connections are established through the exchange of beacon messages among sensor nodes. Equation (3) elucidates the fundamental dynamics of the acyclic connectivity model. Following the principles of acyclic graph connectivity, sensor nodes within the WSN can be configured with associativity rules. The cost of forwarding path is expressed in Eq. 2.

$$cost_{fn} = \begin{Bmatrix} \frac{dist_{src} - dist_{dest}}{dist_n} \end{Bmatrix} \quad \text{Eq. 2}$$

Where $cost_{fn}$, denotes cost function. $dist_{src}$ represents source distance and $dist_{dest}$ symbolizes destination distance. $dist_n$ represents distance of all active nodes (n).

The channel bias indicator is represents in Eq. 3.

$$Set_N \propto Ch_N \quad \text{Eq. 3}$$

Where Ch_N denotes the channel bias factor. Equation (4) illustrates the correlation between 'd' and the channel bias factor, denoted as Ch_N, when the node Set_N remains consistently associated with the channel between a source node and a destination node. This relationship highlights that the channel bias factor directly influences the adjustments made to the subsequent node's association process within the ODAC mechanism. The connectivity between sensor

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

nodes can be disrupted by various types of attackers. An attacker, defined as a sensor node capable of intercepting medium data frames and other control messages, is characterized by the attacker model presented in Eq. 4.

$$Ch^{atck} = frame_i - atck_{fn}(\nabla frame_i . interrup^{fn}(legit_{fr}, target_{fr}) \quad \text{Eq. 4}$$

Where Ch^{atck} represents channel attack, $frame_i$ denotes frame of ith node which is going transmit to destination node. $atck_{fn}$ signifies the attack function and $interrup^{fn}$ means interrupt function. Legit frames are denoted as $legit_{fr}$and $target_{fr}$ represents target frame. Through these Equations, the interleaved honeypot frames are formed. The proposed interleaved honeypot frames is presented in Fig. 3.

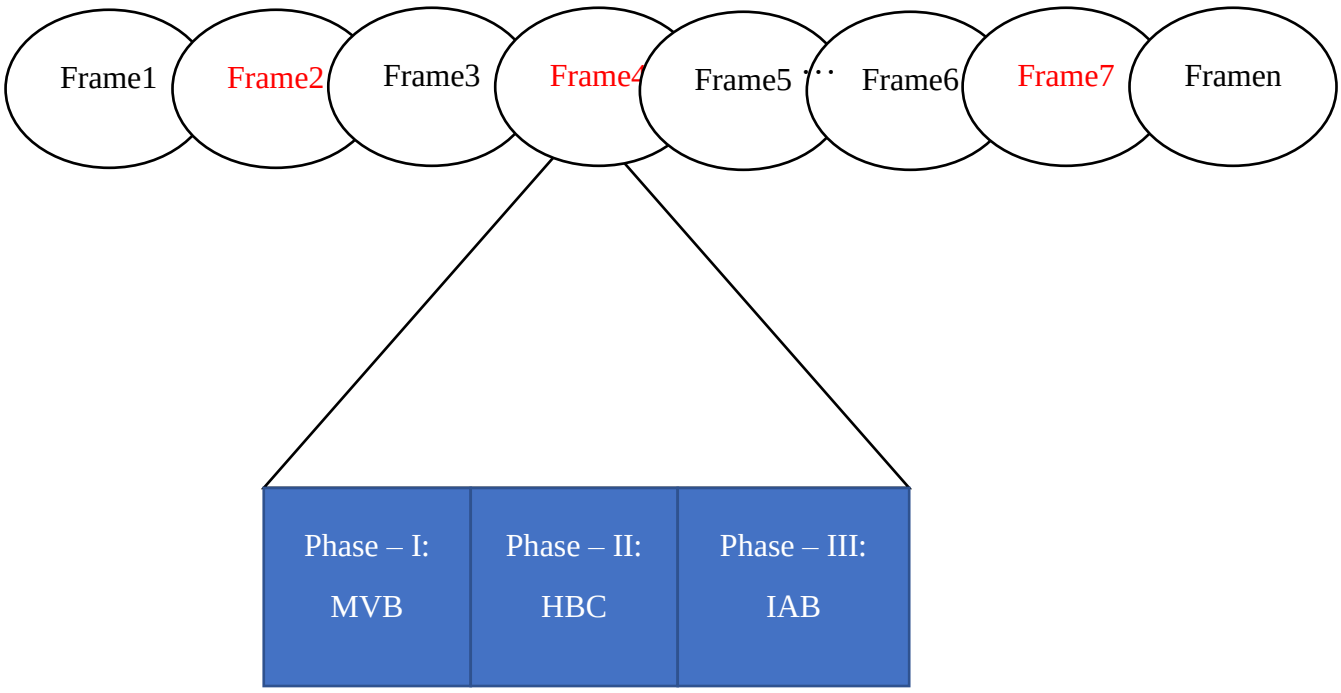

Figure 3. Proposed Interleaved Honeypot Frames

When accessing the honeypot frame instead of an original data frame, each MAC frame sequence incorporates randomly inserted honeypot frames to deceive potential attackers, creating the illusion that they are accessing genuine frame contents. The interleaved honeypot frame comprises an internal Message Validity Block (MVB), Honeypot Boot Block (HBC), and Intrusion Analysis and Validation Block (IVB). As depicted in Figure 3, the MVB furnishes fake frame attributes designed to attract attackers and the incoming frame validity analyzer. Considered as an attacker's request injected into the transmission sequence, the incoming frame undergoes scrutiny by the frame validity analyzer unit within the MVB. This unit assesses the time validity and response expectations associated with attacker injections. Concurrently, each MVB maintains the local node's timestamp value, T(s), indicative of the time of the attacker's injection. Following Figure 3, the Honeypot Boot Block (HBC) serves as a snippet of boot code responsible for initiating the internal honeypot engine functions aimed at detecting attacker events. Serving as a preview of honeypot attack detection functions, the IVB activates intrusion and attack classification procedures to generate malicious logs and alert messages. Typically, the random sequences of IHF function as traps that remain unknown to attackers, thereby enhancing the effectiveness of the honeypot-based security mechanism.

The suggested approach involves implementing a honeypot frame insertion technique using a frame-interleaving algorithm at the sender's end. When transmitting data over a wireless medium, a sender node activates this algorithm. Illustrated in Fig. 4, each sender utilizes an internal honeypot frame queue to store fake frames (honeypot frames). Through the proposed insertion method, the wireless MAC protocol transmits data containing these honeypot-inserted frames, thereby creating a randomized trap for potential malicious injections. Likewise, the receiver node receives interleaved frame sequences and employs a honeypot frame-de-interleaving algorithm to

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

extract the original data. This method ensures secure data transmission, enhancing wireless honeypot security by providing resilience and flexibility.

The process of implementing random honeypot slot generation involves two procedures, A and B, each offering distinct approaches. Procedure A initiates with the generation of a random bit string, leveraging the sender's internal node attributes and employing SHA-3 (512 Bit) computations to ensure unpredictability. Subsequently, a random bit elector function is devised to select bits from the SHA-3 output, maintaining randomness. This approach guarantees absolute slot randomness in honeypot frame insertions rewrite without plagiarizing existing patterns. On the other hand, Procedure B outlines a comprehensive implementation strategy. It begins with defining parameters and constraints, followed by designing a random bit string generation algorithm incorporating SHA-3 computations. A mechanism for selecting random bits from the hash output is developed, ensuring unpredictability. Integration with honeypot frame insertion process and thorough testing validate the randomness and effectiveness of the solution. Whether following Procedure A or B, the objective remains the same: to implement a secure and randomly generated honeypot slot mechanism.

After Procedure $rand_{slot}$, as illustrated in Algorithm 1, the sender node generates random slot identifiers, represented as a sequence of keyed bit strings $random_{slot}(src)$ in a compact tuple key_{str}. Following this, Procedure $IHF_{insertion}$, detailed in Algorithm 2, elucidates the technical intricacies of IHF production and their subsequent insertion into the sender's transmission lines, denoted as $n(trans_{sender})$. Within the context of WSNs, each sender maintains an IHF queue denoted as $IHFQ_{sender}$, ensuring secure multi-path data transmission. In this scenario, the $random_{slot}(src)$ values undergo evaluation by a node-centric parity bit engine to discern true and false cases for IHF insertion into $n(trans_{sender})$. Eq. 5 illustrates key_{str} in matrix format, while Eq. 6 demonstrates the generation of $parity_{bits}$ for IHF insertion between original wireless frames.

Algorithm 1. Procedure $rand_{slot}$
Procedure $rand_{slot}$: gen $rand_{slot}(no, seed)$
Input: $(no, seed)$
Output: $(random\ number, R_{no})$
1. Get $node_n$ MAC Address (48 bits), no
2. Set random seed matrix = $seed(src, key)$
3. Compute, $seed$: $seed \forall src(channel_{id}, session_{id})$
$$seed = no \| \| seed(src * k)$$
$$random\ number_{src} = no \| \| time_{stamp} \| \| Nonce$$
4. Call SHA-3 (512 bits) fn
$R_{no} = {sha_3}^{512}(random\ number)$
$$R_{no}(bin_{bit}) = Bit\ trunc(R_{no})$$
5. Redo upto all src node is computed
6. Construct matrix using $R_{no}(bin_{bit})$
7. Generate random slot $R_{no} = rand_{elect}(R_{no}(bin_{bit}))$
8. Store $random_{slot}(src)$ in key_{str} for each process.
9. Recall
End Procedure $rand_{slot}$

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

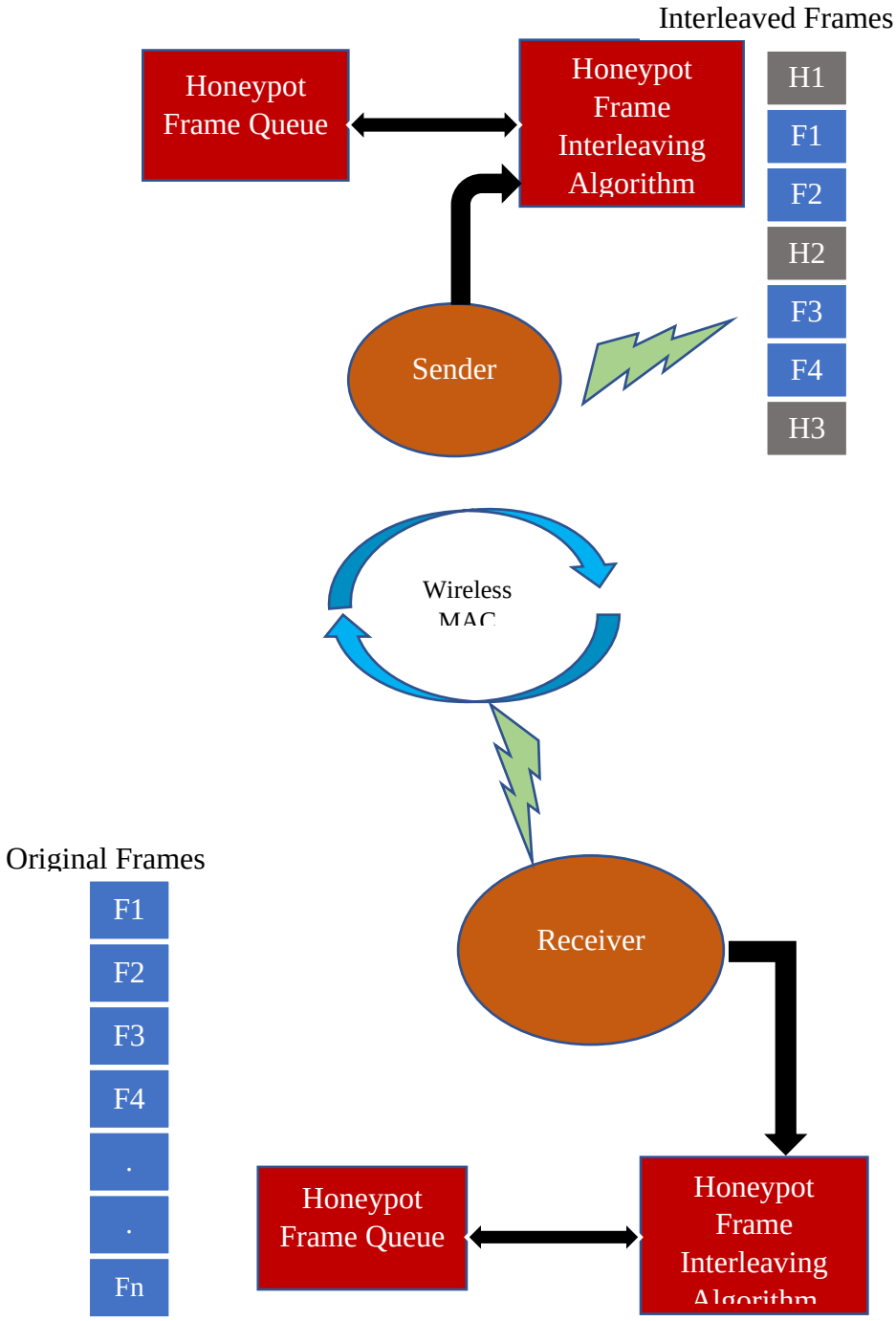

Figure 4. Honeypot frame-interleaving and de-interleaving process.

Algorithm 2. Procedure $IHF_{insertion}$
Input: $random_{slot}(src)$
Output: Interleaved Honeypot Frames
1. Set src to transmission mode
2. Ge$random_{slot}(src)$t in Procedure $fn_{inter}(random_{slot}(src), IHF)$
3. Set IHF Queue $IHFQ_{sender}$

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Do:
For each transmission n($trans_{sender}$) sender
If $random_{slot}$(src) = = P(1)):
POP ($random_{slot}$) & count($random_{slot}$)
Insert (f_n, f_{n+1}, IHF_{src}) → $n(trans_{sender})$
If ($random_{slot}$(src) = = P(0)):
$Insert\ f_n \rightarrow n(trans_{sender})$
Else:
$n(trans_{sender}) \rightarrow Error$
5. Set DHF Queue $DHFQ_{receiver}$
6. Do $n(trans_{receiver})$ at receiver:
If $random_{slot}$(src) = = 1:
POP (f_n, f_{n+1}, IHF_{src})&$push\ (DHFQ_{receiver})$
$(DHFQ_{receiver})cnt^{++}$
If $random_{slot}$(src) = = 0:
$n(trans_{receiver}) \rightarrow Receiveframe$
Else:
$n(trans_{receiver}) \rightarrow Error$
7. Do for all ch_{id}
8. Call Procedure $rand_{slot}$ for each n($trans_{sender}$) and ch_{id}
End Procedure $IHF_{insertion}$

The computation of parity bits is crucial for managing bit-level similarity between the sender and receiver sides based on the sequence of contiguous bit strings. The node-centric parity-checker function is responsible for identifying odd parity combinations within the bit strings, facilitating the insertion of frames. By detecting these odd parity combinations, the function ensures that frames are strategically inserted to maintain data integrity and enhance security during transmission.

$$key_{str} = \begin{pmatrix} 1 & 0 & 0 & 1\cdots & 1 \\ 0 & 0 & 0 & 1\cdots & 1 \\ 1 & 0 & 1 & 1\cdots & 1 \end{pmatrix} \begin{matrix} 0 \\ 1 \\ 1 \end{matrix} \quad Eq.5$$

$$parity_{bits}(0|1) = \sum_{n} key_{str}\,(src, key) \quad Eq.6$$

In WSNs, numerous open channels are accessible for transmitting sensor data. However, these active channels often face threats from malicious activities. In response to this challenge, the proposed system implements IHF solutions across all active wireless channels. By deploying IHF solutions, the system aims to detect and mitigate malicious activities, thereby enhancing the security and reliability of data transmission in WSNs.

In combating malicious attacks and suspicious injections on wireless channels, Intrusion Honeypot Frames (ICFs) play a pivotal role. In WSNs, where data is distributed from various sender nodes through multi-path-routing procedures, there arises a necessity for sender-originated IHFs to counter potential threats. During this process, each IHF is equipped with a random assortment of fake data and other network credentials resembling legitimate ones. This strategic deployment of IHFs aims to deter attackers by presenting them with deceptive targets, thereby bolstering the network's defenses against malicious activities.

Simultaneously, at the sender point and receiver point, interleaving and de-interleaving functions are invoked, respectively. These functions are integral to the data transmission process, ensuring efficient handling of data streams. Data-forwarding nodes and the neighboring nodes of both sender and receiver are involved in exchanging data without accessing or extracting the contents. Meanwhile, the activation of the node-centric honeypot-based

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

DIDS engine relies on successful malicious access to random IHF on the channel. The proposed system implements locally reactive honeypot DIDS engines in each sensor node to counteract potential attacker events. These honeypot DIDS procedures are triggered by the activation of the Honeypot-Based Countermeasure (HBC) in response to attackers' attempts to interfere with IHFs. Procedure $IDS\_Engine(HBC\ and\ IVB)$ (Algorithm 3) delineates the implementation of secure wireless MAC practices based on IHF usage and node-centric honeypot DIDS calls, ensuring robust security measures against malicious activities. Based on the successful execution of the HBC and IVB functions, the security internals of the sensor node invoke Procedure D, as depicted in Procedure $IDS\_Engine(HBC\ and\ IVB)$ (Algorithm 3) . Procedure D is responsible for initiating the event analysis function for each channel transmission occurring across various active intervals. Within this traffic analysis procedure, each request originating from various internal nodes undergoes validation in accordance with Rule Set. This validation process is aimed at detecting intrusions over the channel, thereby enhancing the overall security posture of the network.

Algorithm 3. Procedure $IDS\_Engine(HBC\ and\ IVB)$
Input: $attck_{access}(mac_{src}), Data(mac_{src})$
Output: $attck_{access}, attck_{report}, sus\_evnt_{dtct}$
1. Do for all $attck_{access}(mac_{src})$, If$((attck_{access}(mac_{src}), IHF_{src}) == TRUE$: Go to step 2 If$((attck_{access}(mac_{src}), IHF_{src}) == FALSE$: Go to step 3 2. Call $IDS\_Engine(HBC\ and\ IVB)fn$: Set node intrusion dataset $intr_{ds}$ Get $ev(attck_{access}(mac_{src}))$ at $node_i$ If $(attck_{access}(mac_{src}), IHF_{src}) == TRUE$: Start $ule\ set(traffic_{attr})$; Validate If$((mac_{src}(node_i)) == TRUE$ Validate If $(mac_{src}(parity_{bits}(node_i))) == (mac_{src}(prec(node_i)))$ Validate If $(blk_{id}(parity_{bits}(node_i))) == (blk_{id}(prec(node_i)))$ Start $ch_{rcfn} = \sum_{i=1}^{N} f(ch_1, ch_2, ch_3 \dots \dots .. ch_n) \forall ch_{id}$ Create alert to all nodes $alert_{node}$ Make attacker entry record $attck_{entry}$ Set event classifier logs for each node Update the logs for each session Redo for all channels 3. Continue n($trans_{sender}$) and $n(trans_{receiver})$ 4. Do for all ch_{id} 5. Call Procedure $rand_{slot}$ and Procedure $IHF_{insertion}$ for each n($trans_{sender}$) and ch_{id}
End Procedure $IDS\_Engine(HBC\ and\ IVB)$

The rule-based attack classifiers analyze requests from sensor nodes at the receiver node, contingent upon successful access to IHF by any potential attacker node. Typically, legitimate sensor nodes are barred from accessing IHF, as they primarily engage in interleaving functions. As discussed technically in the proposed model, novel wireless IHF techniques emerge as more dependable security solutions. Nonetheless, the absence of confidentiality, authentication, and channel-sealing policies exposes channels to vulnerabilities against critical wireless attacks. In such circumstances, lightweight encryption algorithms and authentication mechanisms play a crucial role in

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

safeguarding multi-channel data transmissions. To address this, the proposed system introduces channel-aware Advanced Encryption Standard (AES) and Elliptic Curve Cryptography with Digital Signature (ECCDS) algorithms to fortify the security of data on the channel. These algorithms ensure the confidentiality, authentication, and integrity of data transmitted across wireless channels, thereby enhancing the overall security posture of the system.

EXPERIMENTAL RESULTS

The experimental setup is based on the technical specifications outlined in Table 2. In the configured network environment, data communication occurs through multi-hop channels. In this neighbor-based mode, each sensor node functions as a source, destination, or forwarding node. The WSN comprises a maximum of 300 sensor nodes under the most populated scenario. The simulation specifications highlight the significant contributions of HFM-HMAC and ODAC in managing virtual wireless channel policies and IHF policies, respectively. Additionally, the experiment employs a routing fusion approach involving an AODV. protocols to manage multi-channel routing. The WSN nodes are configured with a random mobility model, with velocities ranging between 10 m/s and 50 m/s. Both legitimate network nodes and attacker nodes are allowed to create vulnerable channel conditions in the experiment.

Table 2. Proposed Simulaiton parameters

Parameter	Value
Simulator	NS-3.35
Number of Sensor Nodes	300
Network Area	1000 m × 1000 m
MAC	IEEE 802.11
Channel Type	Wireless
Virtual Backbone	ODAC
MAC Security	HFM-HMAC (Proposed)
Data Traffic	Variable Bit Rate (VBR)
Signal Propagation	Two Ray Ground
Initial Energy (Joules)	50 J
Transmission Range	150 meters
Channel Frequency (GHz)	2.4
Mobility Rate (m/s)	10, 20, 30, 40, 50
Antenna Model	Omnidirectional
Routing Protocol	AODV
Simulation Time (s)	600

In the simulation environment designed for a worst-case WSN scenario within a 1000 m X 1000 m area, deploying 300 sensor nodes with a random mobility model introduces complexity in population density, channel establishment time, and link management. Typically, the maximum transmission range of a sensor node is set to 100 m, but in this scenario, it's increased to 150 m to mimic real-time sensor performance accurately. A constant position mobility model could be used, but it introduces uncertainties and random link/channel constructions in each simulation iteration, offering a better understanding of system performance under varied geographical conditions.

The experimental setup anticipates several types of attackers: wormhole, packet-dropping, identity theft, MAC frame eavesdropping, and misrouting attackers. These attackers are instantiated from selected nodes to launch malicious events randomly, as per the simulation configuration. Wormhole nodes record neighboring node data and tunnel it to another node, while packet-dropping attackers collect data from legitimate nodes and discard it upon receipt. Identity theft attackers manipulate neighbor identifiers due to their lack of network reputation. Eavesdropping attacks record nearby data transmissions, and misrouting attackers alter legitimate routing table entries. Legitimate sensor nodes are expected to intercept any attacks via the wireless channel.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The network simulation is implemented using Network Simulator (NS-3.35), with network setup and data transmission scenarios coded in C++. Internal functions of existing techniques and proposed models are developed using Python library files. The proposed model is compared with existing techniques like WIHFM, LSTM-MAC, PMAC_WSN and RECTANGLE within the NS-3 tool, considering the specified network environment and features outlined in Table 1. This evaluation assesses each technique's contribution against uniform network conditions, providing meaningful insights. Figure 8 illustrates the production latency (in milliseconds) of WIHF in the wireless channel, showing reasonable latency values across different sessions (T1, T2, T3, T4 and T5) when transforming IHFs into legitimate frames.

Fig. 5 illustrates the fluctuation in IHF production latency, ranging from 100 milliseconds (MSec) to 180 msec. The IHF production latency observation indicates the mean duration required to generate and incorporate IHFs into a valid MAC frame sequence across the channel spectrum. The graph presents the average IHF production latency across six observed channels.

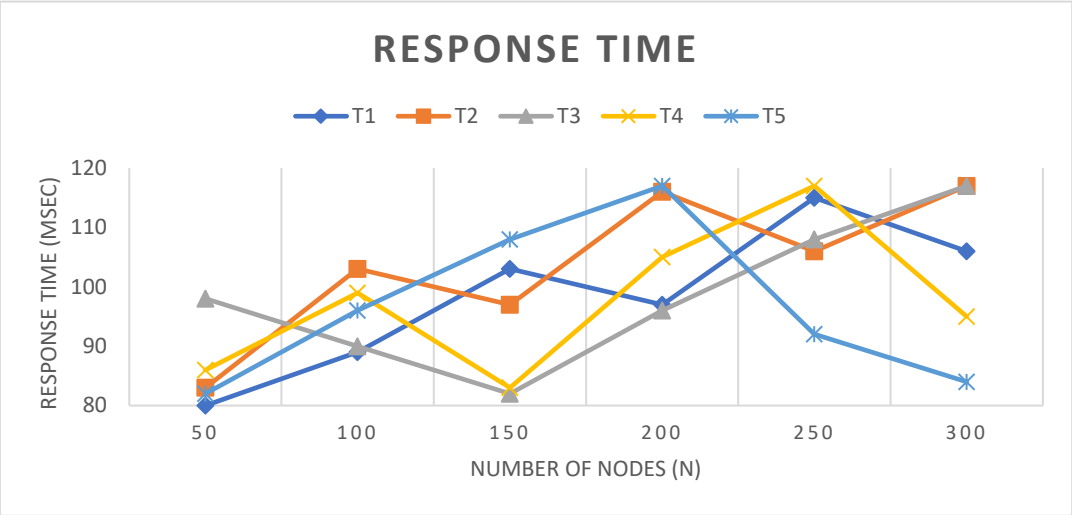

Figure 5. Fluctuation in IHF production latency

The functionality and responsiveness of honeypot engines are essential for ensuring efficient reactive intrusion detection in WSNs. According to Figure 6, the average response time of honeypots spans from 70 msec to 110 msec. This variation in response time is influenced by the idleness rate or multiprocessing rate of each sensor node at time *'T'*.

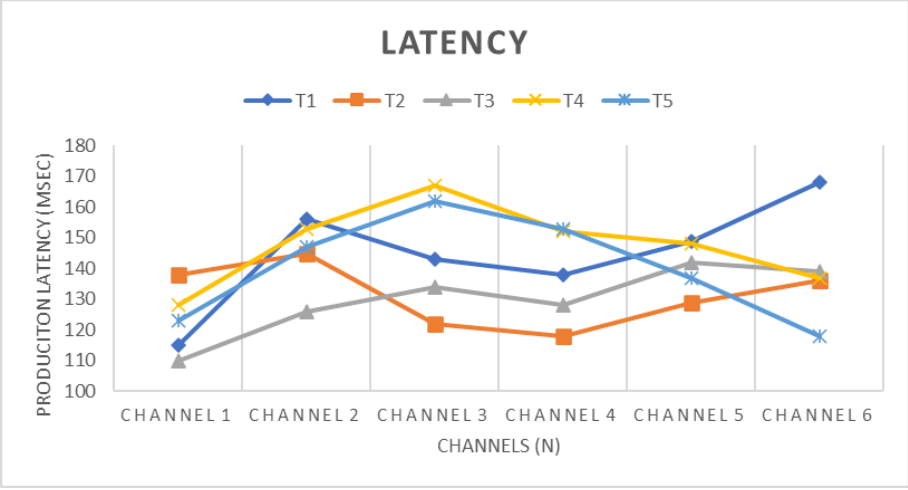

Figure 6. Honeypot Response Time

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Illustrated in Fig. 6, the response time gradually rises with the increasing number of sensor nodes during iterative slots. This increase in nodes contributes to heightened channel liveliness and multiprocessing heaps overall.

Fig. 7 elucidates the average routing delay for each data transmission during vulnerable channel activities. As mentioned, the proposed model boasts a superior honeypot management system characterized by limited latency rates. Moreover, the integration of AODV facilitates swift route updates during interactions with attackers.

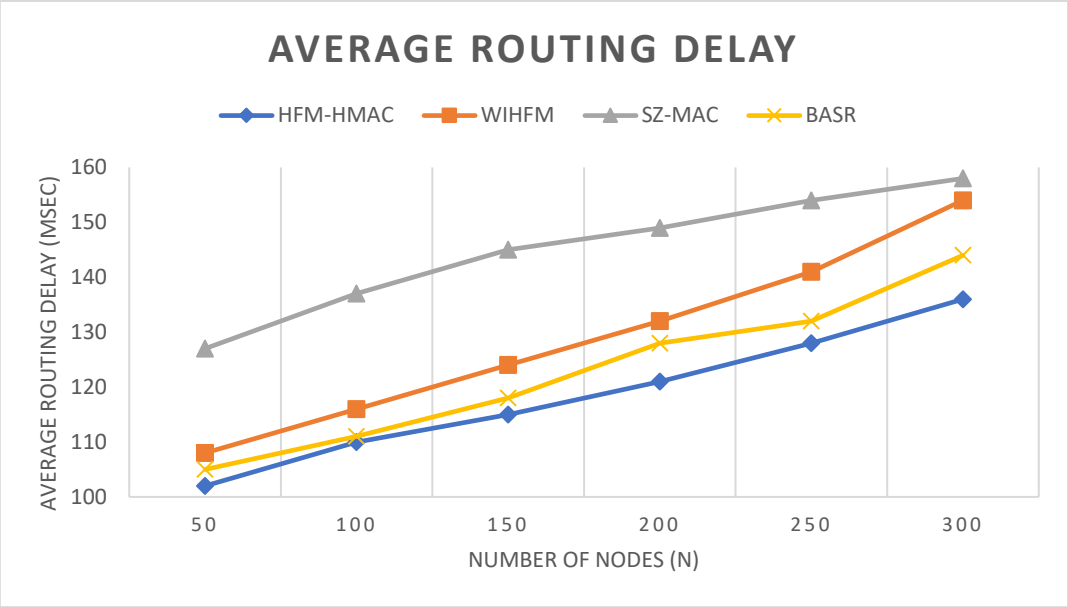

Figure 7. Average Routing Delay

This routing strategy utilizes AODV to enhance reactive route updates and minimize network latencies. Leveraging distributed HFM-HMAC functions, it aims to achieve optimal routing fusion, ensuring minimal routing delays compared to alternative techniques. Within this context, the exploration of a secure and trusted routing protocol emerges as a significant area for further research. Figure 8 illustrates the extra computational load imposed on each node as a result of the complete HFM-HMAC functions alongside other security functions currently in place.

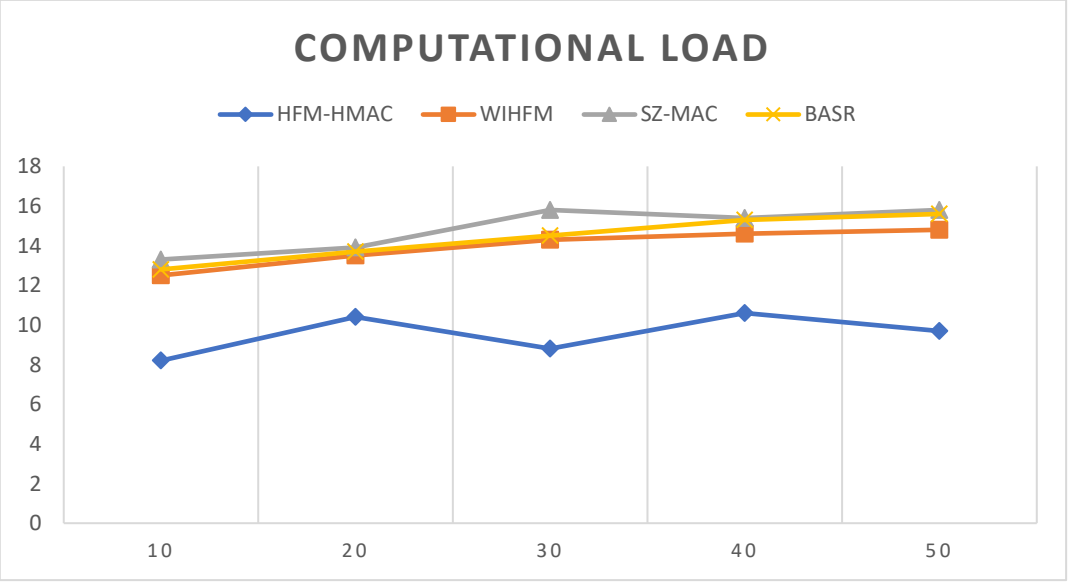

Figure 8. Computational Load

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The suggested functional components of each security method entail a notable computation overhead ranging from 8% to 10.6%. In contrast, the proposed model demonstrates enhanced efficiency in overhead, showcasing improvements ranging from 12.5% to 14.8% compared to alternative techniques. For instance, SZ-MAC reaches its peak overhead at 15.8%, while BASR achieves 15.6%. The proposed model distinguishes itself through lightweight IHF procedures, distributed honeypot management principles, and node-specific attack detection rules. Consequently, the HFM-HMAC approach effectively minimizes computation overhead, particularly as the velocity of sensor nodes fluctuates between 10 m/s and 50 m/s.

Moreover, the proposed HFM-HMAC holds promise for enhancing moderate security platforms and applications. Specifically, its application in WSNs utilized in home automation and agriculture systems, which often demand moderate or minimal security measures, is particularly relevant. In such environments, the HFM-HMAC alongside distributed security policies effectively safeguards network devices, such as sensor nodes, against external intrusions or attacks.

Noteworthy is the HFM-HMAC's performance in scenarios requiring minimal security considerations, where it consistently achieves the maximum specificity and sensitivity rates. Furthermore, sensor nodes employed in agricultural and home automation networks must possess adequate computational capabilities to attain maximum secure throughput rates across channels. The efficiency of computation and power consumption significantly influences the successful implementation of HFM-HMAC procedures in each sensor node.

Consequently, the application of the proposed HFM-HMAC necessitates validation processes tailored to the environment and configuration to ensure optimal energy consumption, latency, throughput, sensitivity, and specificity in real-time operations.

CONCLUSION

The security principles and cryptographic mechanisms employed for safeguarding data communications are commonly utilized across various wireless networks. However, the identification of a novel MAC security management system is essential to bolster WSN resilience against diverse attackers. This article presents the implementation of a distributed HFM-HMAC system, which introduces innovative features.

In this newly developed model, IHF functionalities emerge as novel distributed solutions integrated into each sensor node of the WSN. Moreover, the HFM-HMAC facilitates IHF computations and deploys distributed wireless honeypot engines to create random attacker traps, enticing attackers into counterfeit honeypot resources within sensor nodes. By leveraging this model, attackers and malicious activities are effectively ensnared in IHFs, enabling the identification of intrusion attempts or attacks.

Comparative analysis against existing frameworks like WIHFM, SZ-MAC, and BASR in the experimental section highlights the superiority of the proposed HFM-HMAC across various performance metrics. However, it's worth noting that HFM-HMAC exhibits limitations concerning uncertain IHF latency and honeypot response times, especially as network dynamics undergo continuous changes.

Future technical advancements, including intelligent network dynamic analysis models, dynamic programming models, and uncertainty computation models, are expected to mitigate these limitations. Given the current inadequacy of network MAC models in efficiently handling channel uncertainties with low-powered dynamic programming solutions, improving the static limitations of HFM-HMAC becomes imperative.

Moreover, the evolution of next-generation honeypot solutions in the wireless domain is anticipated to incorporate enhanced distributed trap management policies tailored for application-specific sensor platforms. Considering the energy utilization sensitivity inherent in next-generation WSN models across various application domains, including military and healthcare sensor networks, the proposed novel HFM-HMAC holds promise for exclusive deployment strategies in the future.

REFRENCES

[1] Lloret, J., Garcia, M., Bri, D., & Sendra, S. (2009). A wireless sensor network deployment for rural and forest fire detection and verification. sensors, 9(11), 8722-8747.

Research Article

[2] Mezrag, F., Bitam, S., & Mellouk, A. (2022). An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. Journal of Network and Computer Applications, 200, 103282.
[3] Guimaraes, G., Souto, E., Sadok, D., & Kelner, J. (2005, August). Evaluation of security mechanisms in wireless sensor networks. In 2005 Systems Communications (ICW'05, ICHSN'05, ICMCS'05, SENET'05) (pp. 428-433). IEEE.
[4] Sharma, K., Ghose, M. K., Kumar, D., Singh, R. P. K., & Pandey, V. K. (2010). A comparative study of various security approaches used in wireless sensor networks. International journal of advanced science and technology, 17(2), 31-44.
[5] Bhushan, B., & Sahoo, G. (2020). Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. Handbook of computer networks and cyber security: principles and paradigms, 683-713.
[6] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature Review. Sensors, 22(6), 2087.
[7] Han, Y., Hu, H., & Guo, Y. (2022). Energy-aware and trust-based secure routing protocol for wireless sensor networks Using adaptive genetic algorithm. IEEE Access, 10, 11538-11550.
[8] Soundararajan, R., Rajagopal, M., Muthuramalingam, A., Hossain, E., & Lloret, J. (2022). Interleaved Honeypot-Framing Model with Secure MAC Policies for Wireless Sensor Networks. Sensors, 22(20), 8046.
[9] Rajasoundaran, S., Kumar, S. S., Selvi, M., Thangaramya, K., & Arputharaj, K. (2024). Secure optimized intrusion detection scheme using LSTM-MAC principles underwater wireless Networks. Wireless Networks, 30(1), 209 231.
[10] Palmieri, N., & Campoverde, L. M. S. (2023, June). A MAC layer analysis of an impersonation attack in a wireless sensor network. In Autonomous Systems: Sensors, Processing and Security for Ground, Air, Sea, and Space Vehicles Infrastructure 2023 (Vol. 12540, pp. 202-207). SPIE.
[11] Panahi, U., & Bayılmış, C. (2023). Enabling secure data transmission for wireless sensor networks based IoT applications. Ain Shams Engineering Journal, 14(2), 101866.
[12] Shrivastava, A., Nayak, C. K., Dilip, R., Samal, S. R., Rout, S., & Ashfaque, S. M. (2023). Automatic robotic
[13] system design and development for vertical hydroponic farming using IoT and big data analysis. Materials Today: Proceedings, 80, 3546-3553.
[14] Al Mamun, A., Naznen, F., Jingzu, G., & Yang, Q. (2023). Predicting the intention and adoption of hydroponic farming among Chinese urbanites. Heliyon, 9(3).
[15] Sela Saldinger, S., Rodov, V., Kenigsbuch, D., & Bar-Tal, A. (2023). Hydroponic agriculture and microbial safety of vegetables: promises, challenges, and solutions. Horticulturae, 9(1), 51.
[16] Mamatha, V., & Kavitha, J. C. (2023). Machine learning based crop growth management in greenhouse environment using hydroponics farming techniques. Measurement: Sensors, 25, 100665.
[17] Nikolov, N. V., Atanasov, A. Z., Evstatiev, B. I., Vladut, V. N., & Biris, S. S. (2023). Design of a Small-Scale Hydroponic System for Indoor Farming of Leafy Vegetables. Agriculture, 13(6), 1191.
[18] Gao, J., Al Mamun, A., Yang, Q., Rahman, M. K., & Masud, M. M. (2024). Environmental and health values, beliefs, norms compatibility on intention adopt hydroponic farming among unemployed youth. Scientific Reports, 14(1), 1592.
[19] Goh, Y. S., Hum, Y. C., Lee, Y. L., Lai, K. W., Yap, W. S., & Tee, Y. K. (2023). A meta-analysis: Food production and vegetable crop yields of hydroponics. Scientia Horticulturae, 321, 112339.
[20] Dhawi, F. (2023). The role of plant growth-promoting microorganisms (PGPMs) and their feasibility in hydroponics and vertical farming. Metabolites, 13(2), 247.
[21] Kaur, G., Upadhyaya, P., & Chawla, P. (2023). Comparative analysis of IoT-based controlled environment and uncontrolled environment plant growth monitoring system for hydroponic indoor verticalfarm. Environmental Research, 222, 115313.
[22] Trisnasari, W., & Saridewi, T. R. (2023). Smart Greenhouse Technology for Hydroponic Farming: Is it Viable and Profitable Business?. International Journal on Advanced Science, Engineering & Information Technology, 13(4).

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[23] Hikmah, N., & Susanti, A. (2023). Analysis Of Economic Opportunities For Farming With Hydroponic Systems In Makassar City. Jurnal Manajemen Bisnis, 10(2), 392-405.
[24] Venu, S., & Muralimohan, G. (2023, July). Sustainable atmospheric water generator for hydroponic farming. In AIP Conference Proceedings (Vol. 2788, No. 1). AIP Publishing.
[25] Niswar, M. (2024). Design and Implementation of an Automated Indoor Hydroponic Farming System Based on the Internet of Things. International Journal of Computing and Digital Systems, 15(1), 337-346.
[26] Falah, M. Z., Handoko, W. T., Syah, A. I., Azizah, F. Z., & Gumilar, L. (2023). Implementation of smart farming based solar cell system in hydroponic in the agricultural area of blitar village. Community Development Journal: Jurnal Pengabdian Masyarakat, 4(4), 7015-7020.
[27] Kondaka, L. S., Iyer, R., Jaiswal, S., & Ali, A. (2023, January). A Smart Hydroponic Farming System Using Machine Learning. In 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) (pp. 357-362). IEEE.
[28] Rasyid, A., Yudiandri, T. E., Nurhab, M. I., Papilaya, F., & Heryadi, D. Y. (2023). The Effect of Marketing Mix on Repurchase Intention of Hydroponic Farm Vegetable Products. JEMSI (Jurnal Ekonomi, Manajemen, dan Akuntansi), 9(2), 376-381.