Enhancing IoT Security Using Spider Web-Based Dynamic Keys and Blockchain Encryption)

(تعزيز أمان إنترنت الأشياء باستخدام مفاتيح ديناميكية مستوحاة من شبكة العنكبوت وتشفير سلسلة الكتل

Razan Rezk: Syrian Virtual University _ Damascus _Syria
Wasim Al-Juneidi: Syrian Virtual University _ Damascus _Syria
Corresponding: razanrezk96@gmail.com
Submitted date: 23 August2026 - **Accepted date:** 1 October 2026.

ABSTRACT

The present investigation proposes a novel hybrid security architecture that reconciles robust defense against Denial-of-Service (DoS) attacks with resource-efficient operation within Internet of Things-based wireless sensor networks (IoT-WSNs). The framework synergistically integrates three principal techniques: Spider-Web-based Dynamic Key (SWDK) generation for lightweight cryptographic operations, Principal Component Analysis (PCA) for data dimensionality reduction, and blockchain technology for immutable, tamper-resistant authentication. This model underwent comprehensive evaluation via the NS-3 network simulator, employing a cluster-based topology consisting of one base station and four sink nodes acting as cluster heads, with network densities varying from 3 to 9 sensors per cluster under static node and open-channel assumptions. Performance was assessed under two flooding attack configurations: a distributed, concurrent assault transmitting at 500 packets per second, and a concentrated, high-intensity assault utilizing larger packet sizes (1024 bytes) and escalated rates of up to 1500 packets per second. Empirical findings attest to the pronounced efficacy of the integrated framework; Under distributed attacks, the model curbed the malicious packet delivery ratio to below 14% while attaining a classification accuracy surpassing 93%, thereby reducing the overall attack success rate by 73% to 85%. In the context of concentrated, high-density attacks, although the blockchain layer independently demonstrated only modest resilience, the complete triple-integrated system yielded exceptional latency stabilization, achieving an average reduction of approximately 70% (with observed spanning improvements of 55% to 82%). This security enhancement inherently introduced marginal performance trade-offs, evidenced by a mean throughput decline of roughly 25% and a concomitant reduction in the legitimate Packet Delivery Ratio (PDR). Nevertheless, given the stringent security demands of mission-critical domains such as healthcare and smart infrastructure, this compromise is justifiable. Subsequent research directions should prioritize the optimization of queuing mechanisms, the implementation of adaptive compression protocols, and the periodic renewal of cryptographic key parameters, alongside exploratory efforts toward hardware acceleration and topological scalability.

Keywords: Wireless Sensor Networks (WSNs), Internet of Things (IOT), Data Security Spider Web Dynamic Key, Blockchain, Data Compression, Secure Data Aggregation.

الملخص

تهدف هذه الدراسة إلى تطوير نموذج أمني هجين مبتكر يوازن بين الحماية القوية ضد هجمات حجب الخدمة (DoS) وكفاءة استخدام الموارد في شبكات الاستشعار اللاسلكية لإنترنت الأشياء (IoT–WSN). يدمج الإطار المقترح ثلاث تقنيات رئيسية: توليد المفاتيح الديناميكي القائم على شبكة العنكبوت (SWDK) للتشفير الخفيف، وتحليل مكونات المفاتيح (PCA) لضغط البيانات، وتقنية سلسلة الكتل (Blockchain) للمصادقة المقاومة للتلاعب. تم تقييم النموذج باستخدام محاكي شبكة عالي الدقة (NS–3) ببنية عنقودية تتألف من محطة أساسية مركزية وأربع عقد طرفية (مستقبلات) كرؤوس للعناقيد، مع كثافات شبكية متدرجة (من 3 إلى 9 مستشعرات لكل عنقود) بافتراض عقد ثابتة ونماذج قنوات مفتوحة. تم اختبار النموذج في ظل سيناريوهين لهجوم الفيضان: هجوم موزع متزامن بمعدل 500 حزمة/ثانية، وهجوم مركز بحجم حزمة أكبر (1024 بايت) ومعدل يصل إلى 1500 حزمة/ثانية. أظهرت النتائج كفاءة النموذج الهجين العالية. في بيئة موزعة، نجح النظام في خفض نسبة تسليم الحزم الخبيثة إلى أقل من 14%، وحقق دقة تصنيف تتجاوز 93%، مما أدى إلى انخفاض معدل نجاح الهجمات الإجمالي بنسبة تتراوح بين 73% و85%. أما في الهجمات المركزية عالية الكثافة، فرغم أن أداء تقنية البلوك تشين وحده لم يكن حاسمًا، إلا أن التكامل الثلاثي حقق استقرارًا ممتازًا في زمن الاستجابة، حيث خفض متوسط زمن الاستجابة بنسبة 70% (بين 55% و82%). وعلى الرغم من أن المفاضلة الأمنية أدت إلى انخفاض طفيف في الإنتاجية الإجمالية (حوالي 25%) وانخفاض في معدل تسليم الحزم المشروعة، إلا أن هذا حل وسط مقبول نظرًا لطبيعة التطبيقات الحيوية كالرعاية الصحية والبنية التحتية الذكية. ويوصى بإجراء تحسينات مستقبلية على إدارة قوائم الانتظار، والضغط التكيفي، والتجديد الدوري للمعاملات المشفرة، مع إمكانية تسريعها عبر الأجهزة وزيادة قابليتها للتوسع..

الكلمات المفتاحية:شبكات المستشعرات اللاسلكية (WSNs)، إنترنت الأشياء (IoT)، البنية النجمية (Star Topology)، أمان البيانات، المفتاح الديناميكي لشبكة العنكبوت (SWDK)، سلسلة الكتل (Blockchain)، ضغط البيانات (PCA)، التجميع الآمن للبيانات.

INTRODUCTION

The proliferation of Internet of Things (IoT) technologies, coupled with advances in network speed and data management, has accelerated progress in domains requiring continuous remote monitoring, including smart homes, industrial control, and healthcare services [1]. However, this evolution introduces significant cybersecurity challenges, particularly at the network edge, where sensors and actuators interact directly with the physical environment [2]. With the global number of connected devices projected to surpass 30.9 billion [3], the frequency and sophistication of cyberattacks are escalating, necessitating robust yet lightweight security mechanisms. Traditional encryption and authentication schemes, designed for stable and homogeneous computing environments, are ill-suited to the heterogeneous, resource-constrained nature of modern IoT deployments [4]. This challenge is especially pronounced in Wireless Sensor Networks (WSNs), a prevalent IoT paradigm comprising numerous heterogeneous nodes with limited energy and processing capabilities. The urgency of defending against resource-draining threats, notably Denial-of-Service (DoS) attacks, is paramount. However, excessively complex cryptographic operations accelerate battery depletion and exacerbate communication delays due to packet overhead, underscoring the need for lightweight security strategies to ensure network longevity [5][6][7][8]. To address this gap, the present work proposes a secure architectural framework that integrates lightweight encryption, data compression, and blockchain technology. Specifically, a Spider-Web-inspired Dynamic Key (SWDK) enhances device identification and security, Principal Component Analysis (PCA) reduces transmission overhead by compressing data, and blockchain-based encryption consolidates data integrity and future-proofs the network against adversaries, all while preserving energy efficiency. Scientific Contributions Mutual Triple Integration: The synergistic combination of SWDK, PCA, and Blockchain provides comprehensive protection without imposing excessive resource strain. Attack-Type Sensitivity: The discernible variance in performance between distributed and concentrated attacks provides critical insights for designing adaptive defenses. Practical Viability: The ~70% latency reduction under concentrated attacks meets the stringent requirements of real-time Internet of Things (IoT) applications [9].

Previous studies

About denial of service in wireless sensor networks, Demirci et al [1] proposed a kind of security mechanism meant to spot nodes that are compromised already. Their method looks at packet loss ratios, and also checks both the incoming and outgoing data volumes, while using an improved search routine, TDFS, to trace the attack back from the base station all the way to where it started. After they manage to identify the misbehaving node, its communications are rerouted toward a honeypot, so it can be contained there. Their simulations showed the idea is better than EVO and MULTI, especially in how fast it detects the threat, reaching a detection probability of 0.8 even when the likelihood of a malicious node is only 0.05. Similarly, Al Ebrahim et al. [2] built a machine learning driven framework aimed at identifying and mitigating DoS and DDoS assaults in real time inside software-defined WSNs, meaning SDWSN. Instead of focusing on one single signal, they used traffic related characteristics like packet types, packet sizes, sending rates, source and destination addresses, plus some statistical indicators. Using these features, they trained a classifier to separate normal data flows from adversarial ones. The reported outcomes were striking: the packet delivery fraction rose from 1.45% up to 72.74%, the delay dropped significantly from 12,016 ms down to 297 ms, the detection precision reached 100%, and the approach removed false alarms entirely. As cyberattacks keep getting more sophisticated, a combination of various tactics into one single coherent framework has become way more important, mainly to reduce computational overhead. In that direction, Prasad et al. [10] propose a hybrid plan for WSN DoS detection that uses a joint feature selection optimization idea. It blends the Grasshopper Optimization Algorithm (GOA) and a Genetic Algorithm (GA)—they call it GOA-GA. The whole thing is designed to shrink the feature set you actually need, and then do traffic classification with four separate ML models, namely MLP, KNN, CART, and LR. The goal is to label traffic as either normal or belonging to one of four attack categories, and it's tested on a particular WSN benchmark. In their results, the GOA-GA plus KNN demonstrated the best performance, achieving the highest accuracy of 95.51% with the shortest computation duration too. At the same time, Elumalai et al. [4] came up with a more general intrusion detection framework for WSNs, where they combined a temporal anomaly module—an Autoencoder teamed with a GRU—with a lightweight blockchain. That blockchain uses PBFT and smart contracts, aiming to isolate malicious nodes and update routing tables when needed. Their experiments reported 97.4% accuracy, 2.1% false positives, a 61 ms response time, and 2.4 mj energy consumption per operation. Overall, the reported outcomes look better than approaches that rely only on deep learning, or only on blockchain, or even sys-

tems built purely on learning components without that hybrid balance. Additionally, A. Jawahar et al. [5] put together a combined security architecture, mixing blockchain and ML, for dealing with DDoS attacks in IoT setups. They used customized Random Forest plus SVM models, to do closer traffic pattern scrutiny, then they designed a dedicated blockchain for recording security incidents, and finally they linked both parts with an intelligent integration layer. That layer basically routes the analytic outputs into smart contracts so the system can make quick isolation decisions. With all that, they reported around 94% detection rate, with only about a 3.2% false-positive ratio. Mohamed Anwar and Pavalarajan [6] place extra weight on keeping data intact and private, so they designed a rather advanced encryption setup for IoT networks. In their approach, the key is generated on the fly and it refreshes every time a piece of data is sent, which helps the scheme stay less predictable and more robust, even when someone is trying to sneak in or breach things. On another track, Shakor et al. [7] came up with a security model that works in two phases for cloud storage. Phase one is basically about producing dynamic AES keys, so each individual file ends up being encrypted with a key that keeps shifting. Phase two then leans on blockchain, not just to store those keys but to archive them together with their related metadata too, and at the same time they use ECC protection for the public keys in order to strengthen what happens during both sending and storage. Overall, their plan gives strong cipher coverage, enables decentralized control over the cryptographic keys, blocks unauthorized access, and still stays adaptable, meaning it can grow with the newer and more demanding needs of modern cloud security requirements.Blockchain really does shine as a leading way to plant trust, security, and decentralization inside wireless sensor networks, even if at first glance it looks kind of heavy. Draz et al. [8] introduced a blockchain-backed protocol that helps with energy exchange between nodes in those resource scarce WSNs. Instead of going all in on raw computation, they hinge the whole method on smart contracts plus a lighter consensus approach called Proof-of-Stake (PoS), so the protocol tends to reduce both computational load and energy consumption. Their simulations showed it lowers energy waste and also makes the network more adaptable, extending the service time by about 20% when you compare it with standard solutions. Then, Arachchige et al. [9] presented an IoT security design that uses blockchain specifically to counter DDoS attacks, by deploying a distributed protective mechanism that detects intrusions early and then isolates the affected nodes. In their setup, they didn't use Proof-of-Work, they swapped it out for the more energy conscious Proof-of-Authority. Meanwhile, Rai et al. [11] looked at how blockchain and IoT can come together to strengthen data privacy and security in energy domains, and they especially zoomed in on nuclear power. Their proposal describes a secure information governance structure that ties encryption, integrity checks, and one shared communication framework together. They argue that blockchains built in immutability and transparency, provide solid protection for data overall. Taken as a whole, these investigations kind of converge on the notion that the upcoming security paradigms for IoT and WSN ecosystems will be anchored in hybrid frameworks that somehow synergize cryptographic robustness with blockchain dependability [15]. Crucially, they also keep underscoring the ongoing imperative to minimize computational burdens, ensuring that it stays aligned with the tightly constrained resource environments, typical of these networks [12][13][14].

MATERIALS AND METHODS

The suggested approach puts together a unified framework that integrates dynamic encryption strategies with blockchain driven security. Initially, the data collected from sensor nodes gets protected using a dynamic key created via the Spider Web inspired Dynamic Key (SWDK) method. Even if this key boosts the system's overall safety, it also tends to artificially expand the transmitted packet size, so communication overhead goes up, a bit more than expected. To calm that downside, Principal Component Analysis (PCA) is integrated specifically for data compression, before the information is relayed to the aggregation unit. Then the compressed and encrypted streams coming from several sensors finally meet at a central aggregator, where they are processed together, in a group sense. After that, an extra blockchain encryption layer is added, to further back up data dependability and integrity, so it does not get easily tampered with. The network works with a mesh kind of topology including N nodes and L links. From those, we pick a subset M ($M \in N$) as data aggregation units, using the ones with the highest remaining energy levels. Overall, we can write this as a connected graph, G=(N,L),and it contains three different kinds of nodes, not really more. ***Sensors***: these are the terminal nodes in charge of sensing the surroundings and then forwarding the collected data to the nearest aggregation point, more or less. ***Sinks***: these act like cluster heads, they collect the data coming from the nearby sensors, do some processing and aggregation, and then they relay the combined information to-

CC BY

ward the base station. ***Base station***: it is located at the heart of the network, and it acts as the ultimate sink that receives every aggregated report from the four sink nodes, all of them. The simulation deployment comprises one base station and four distinct clusters, each containing a sink node along with a variable number of sensors ranging from 3 to 9 per cluster. To assess the influence of network size on overall performance and to gauge the proposed framework's adaptability across different densities, the sensor count is adjusted in each simulation trial—covering a spectrum typical of small- to mid-scale wireless sensor networks. The spatial arrangement of nodes remains consistent throughout: the base station is fixed at coordinate (50, 50), the four sinks are located at a uniform distance of 25 meters from the base, and the sensors are evenly distributed in circular patterns with a radius of 10 meters surrounding each sink. While this configuration is somewhat idealized and does not incorporate physical obstructions, it remains sufficiently representative for practical experimental validation.

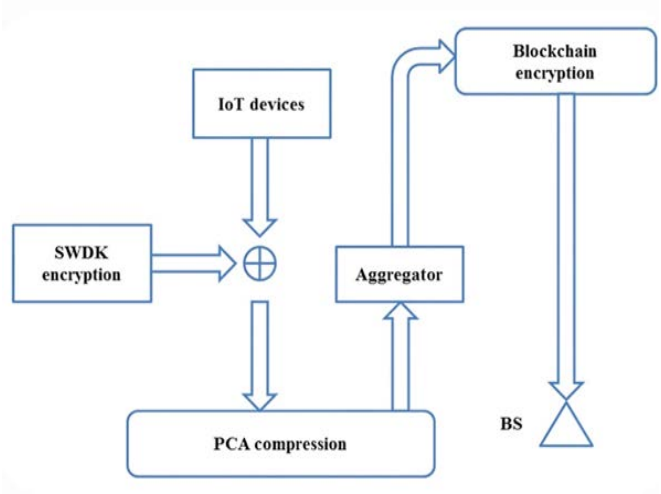


Figure 1: The proposed model

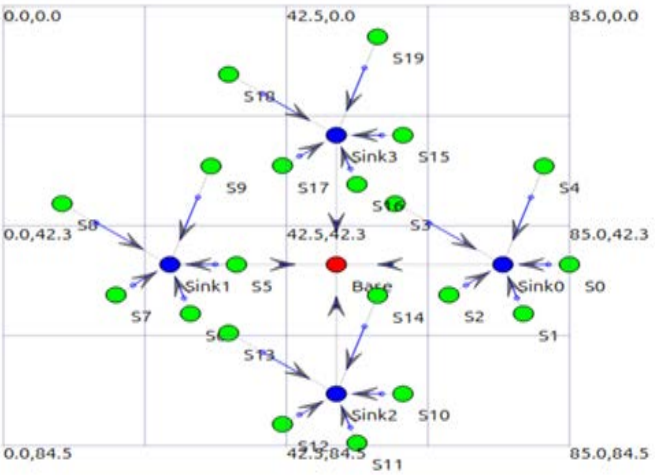


Figure 2: Sensor network topology under investigation.

Dynamic Key Generation (SWDK): The SWDK is derived from the geometrical principles of spiderwebs, yielding an irregular and non uniform structure that offers strong resistance against cryptanalysis and ensures a high security level. The web is composed of radial and spiral strands placed at variable intervals, with their exact offsets governed by configurable parameters—these may incorporate node specific identifiers (such as serial codes or physical positions) to generate diversity across keys. The intersections of these strands define the underlying cryptographic foundation; hence, restoring the key demands thorough familiarity with the parameter set of the Spiderweb Simulation Component (SWC), a model carefully designed to emulate the natural web weaving process of spiders.The key selection process is governed by a set of criteria, namely: a)Data sensitivity and confidentiality: selecting encryption keys appropriate to the sensitivity level of the transmitted data—using stronger keys for highly sensitive data and less robust keys for data with lower sensitivity. b)Susceptibility to attacks: employing dynamic key rotation based on detected attacks. c)Node resource constraints: matching the key to the node's capabilities to ensure no delays occur during data transmission. d)Data category: each data block is classified into a specific category, and a distinct security key is dynamically allocated based on its category and criticality. e)Threat exposure and acceptable risk margins: key selection is based on anticipated threat exposure and the acceptable risk level for each data type.

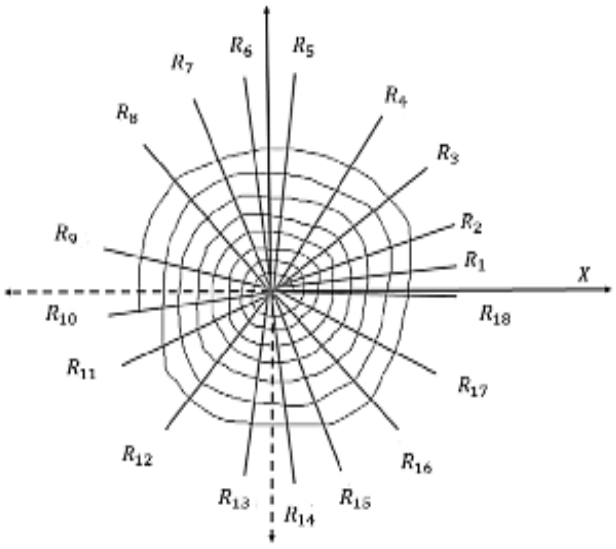


Figure 3:The spiderweb network

The radial lines can be defined by the relation:

$$ad_0 = ad + \Delta ad$$
$$ad_{next} = ad_0 + \Delta ad$$

The spiral lines can be defined by the relation:

$$d_1 = d_{init} + \Delta d$$
$$d_{next} = d_1 + \Delta d$$

The encryption function can be defined by the relation:

$$X'_n = X_n \oplus K_n$$

Principal Component Analysis (PCA): Within the proposed framework, Principal Component Analysis (PCA) fulfills a twofold function: it is deployed either on the raw sensor data matrices at the local node prior to the SWDK-based dynamic encryption, or on the aggregated data matrix structure prior to the key-matching stage:

$$X'_n = X_n \oplus K_n$$

This paradigm leverages PCA's intrinsic capacity to reduce linear dependencies and minimize packet dimensionality, resulting in a marked decrease in network transmission load. Critically, the compression mechanism preserves the integrity of the security model, as the dynamic key's randomness and the ciphertext's decipherability remain entirely intact. The compression operation is formally expressed as:

$$CX'_n = f_c(X'_n) = [{}^{X'_n}_{c}]$$

wherein the ciphertext is supplemented by a compression coefficient. This formulation ensures lossless reconstruction at aggregation nodes while simultaneously achieving enhanced transmission efficiency through reduced in-transit data volumes, without compromising the stipulated security constraints. **Blockchain**: The integration of blockchain technology with Internet of Things (IoT) frameworks constitutes a robust mechanism for safeguarding data integrity and ensuring tamper resistance, as it relies on a distributed ledger architecture that renders any unauthorized modification attempts computationally expensive. Building upon this principle, a private/permissioned blockchain, specifically tailored for clustered wireless sensor network environments, has been adopted. Within this architecture, a lightweight consensus mechanism grounded in Proof-of-Authority (PoA) is distributed among the cluster head nodes (sink nodes) and the base station, with the aim of supporting energy efficiency and significantly reducing response latency compared to conventional protocols such as PBFT or Proof-of-Work. The construction of the blockchain proceeds through a structured multi-stage procedure, which is detailed as follows: Data Segmentation: The aggregated dataset (CX) at the sink node is initially partitioned into j discrete blocks, formally denoted as

$$b_1(CX), b_2(CX), \ldots, b_j(CX)$$

Category-Based Dynamic Encryption: Each data block b_i is subsequently classified into a specific category belonging to the set

$$(Cb_1, Cb_2, \ldots, Cb_n)$$

A distinct security key is then dynamically allocated to each block, contingent upon its designated category and the relative criticality of its contents. This category-aware encryption strategy ensures that stronger cryptographic primitives are assigned to high-sensitivity data segments, whereas shorter key lengths—and consequently, smaller data payloads—are utilized for less critical information. The key selection process is governed by a set of predefined criteria, including data confidentiality requirements, anticipated threat exposure, and acceptable risk margins. Following the assignment and application of the appropriate key, the encryption of the block is finalized. **Blockchain Assembly and Structuring:** For each encrypted block, a final data structure FD_i is constructed, comprising the following four essential components:

Cb_i : The encrypted data payload.

K : The security key employed for encryption.

P : A cryptographic pointer to the preceding block in the chain.

H : The cryptographic hash digest of the current block.

Collectively, these structures form the complete blockchain sequence FD_1,FD_2,...,FD_n, which securely persisted in the database prior to its transmission to the base station. Under this architectural framework, successful reconstruction of the original plain text by an adversarial entity is contingent upon prior access to the dynamically distributed keys, thereby ensuring robust data confidentiality and resilience against unauthorized decryption. **The simulation framework** employed in this study was the NS-3 platform, a high-fidelity environment capable of modeling wireless sensor network behavior with a degree of realism that closely approximates practical deployment scenarios. This platform

CC BY

is particularly well-suited for assessing network robustness against adversarial cyber threats. Two distinct attack classes were emulated through the introduction of malicious nodes configured to inject high-rate packets with spoofed origins. This strategy was designed to exhaust available bandwidth resources and induce queue saturation at both intermediate downstream nodes and the base station (BS). Quantitative performance evaluation under these attack conditions was conducted using the following metrics: **Total Throughput**: Defined as the aggregate volume of data successfully delivered to the destinations, normalized by the total simulation duration, and quantified in kilobits per second (kbps). **Average Delay:** Computed as the mean temporal interval between packet transmission at the source and its successful arrival at the destination. This calculation relies upon a TimestampTag mechanism that records both transmission and reception instants; the difference is subsequently averaged over the total number of successfully received packets. This metric comprehensively encapsulates wireless propagation latency, queuing delays, and processing overhead at the receiver. **Packet Delivery Ratio (PDR):** Determined as the ratio of the number of packets successfully received at their destinations to the total number of packets originating from the sources. **Legitimate Packet Delivery Ratio (Legitimate PDR):** A specific indicator that quantifies the network's capacity to forward authentic data flows in the presence of adversarial activity. **Illegitimate Packet Delivery Ratio (Attack_PDR):** A metric that measures the proportion of maliciously injected packets that successfully traverse the network and reach their intended endpoints. These metrics collectively facilitate a comprehensive and systematic evaluation of the proposed framework's efficacy in mitigating DoS and flooding attacks while preserving reliable communication in resource-constrained sensor network environments. Two distinct attack scenarios were designed to evaluate the resilience of the proposed framework: **Type 1: Concurrent Attack on the Base Station and All Downstream Nodes** In this scenario, three malicious nodes were deployed within a medium sized network a configuration deemed sufficient to assess the attack's impact, while acknowledging that real world deployments may involve varying numbers of adversaries. The attack traffic was generated at a fixed rate of 500 packets per second, distributed uniformly among the base station and the four downstream nodes, corresponding to 100 packets per second directed at each target. This transmission rate, equivalent to approximately 0.5 Mbps, can induce a measurable degradation in Wi Fi network performance. Both legitimate and attack packets were configured with a fixed size of 512 bytes; this standardization was intentionally adopted to isolate the effects of encryption and compression by eliminating packet size variability. **Type 2: Targeted Attack on the Base Station and a Single Sink Node** In the second scenario, three attacking nodes were employed, each transmitting at a rate of 1,000 packets per second to a single sink node and 1,500 packets per second to the base station. These elevated rates are indicative of a high intensity attack. Additionally, the attack packet size was set to 1,024 bytes twice the size of legitimate packets (512 bytes) thereby artificially amplifying the network load.

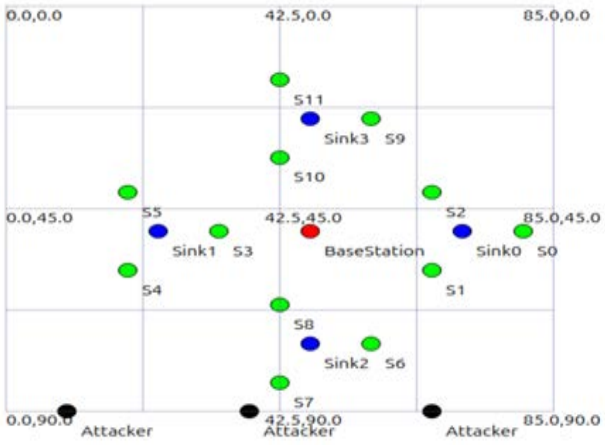


Figure 4: Network nodes and malicious nodes.

RESULTS

Impact of the Attack

An evaluation of the attack's influence on network behavior reveals a pronounced deterioration in Quality of Service (QoS) for legitimate traffic. The attack induces a substantial elevation in end-to-end delay alongside a notable decline in the Packet Delivery Ratio (PDR) for authentic packets. Aggregate throughput registers an increase, attributed to its composition, which accounts for both malicious packets arriving at interfaces and legitimate data. A comparative analysis of the two attack configurations indicates that a focused assault on a single sink induces significantly worse performance in terms of both latency and PDR than a distributed assault across multiple sinks. This is attributable to the complete saturation of the targeted node's ingress port, which generates severe localized congestion.

Performance of Blockchain-Based Protection

Distributed Attack Scenario: Under the distributed attack scenario, the blockchain mechanism demonstrated remarkable effectiveness. It successfully curtailed the proportion of malicious packets reach-

CC BY

ing network interfaces to below 7% and attained classification accuracy exceeding 93%, thereby neutralizing the overwhelming majority of malicious traffic while sustaining relatively modest latency levels. Focused Attack Scenario: Under the concentrated attack scenario, blockchain performance proved less conclusive. Although it reduced the attack success rate relative to an unprotected network configuration, between 25% and 56% of malicious packets still reached their intended targets, with the exact proportion depending on the number of active sensor nodes. This outcome suggests that blockchain in isolation is sufficient for repelling high volume, targeted attacks concentrated on individual ports. Nevertheless, a discernible improvement in end to end latency was observed with blockchain deployment compared to the baseline network under attack. However, latency remained elevated during concentrated attacks, approaching approximately 0.3 seconds.

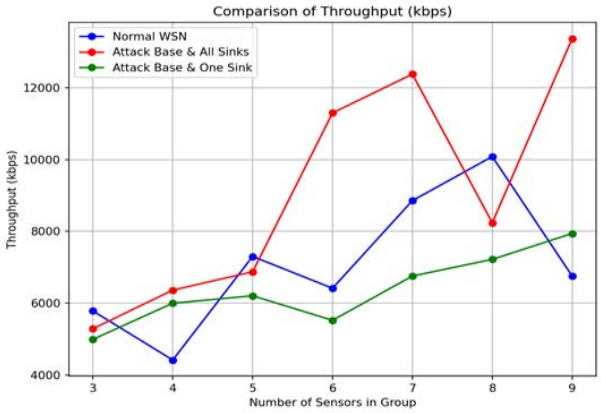


Figure 5: Impact of the attack on throughput.

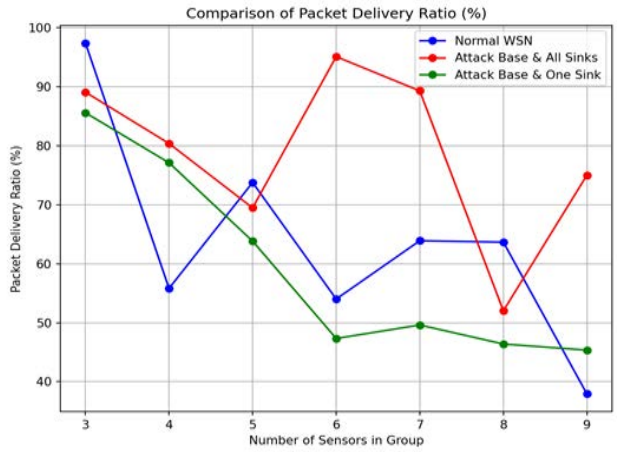


Figure 6: Impact of the attack on packet delivery ratio.

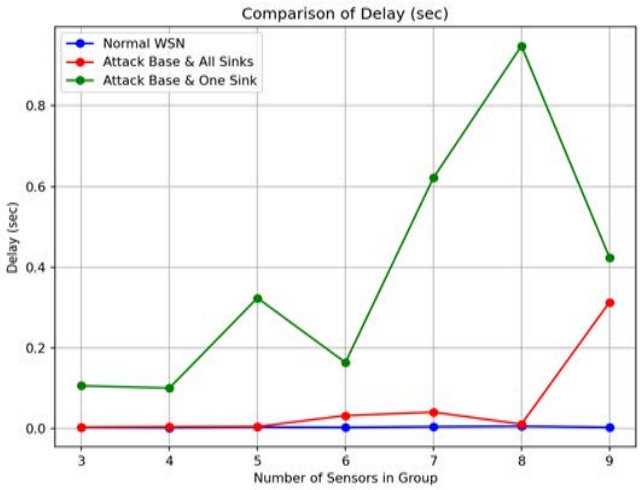


Figure 7: Impact of the attack on packet delivery latency.

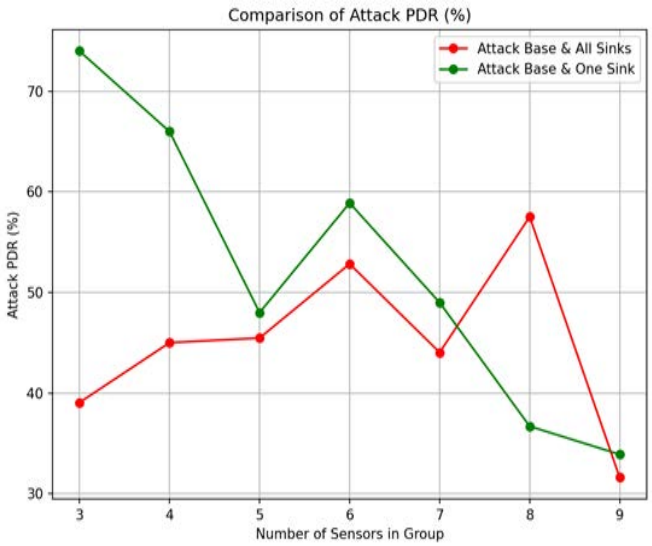


Figure 8:Comparison of packet delivery ratios for the two attack types.

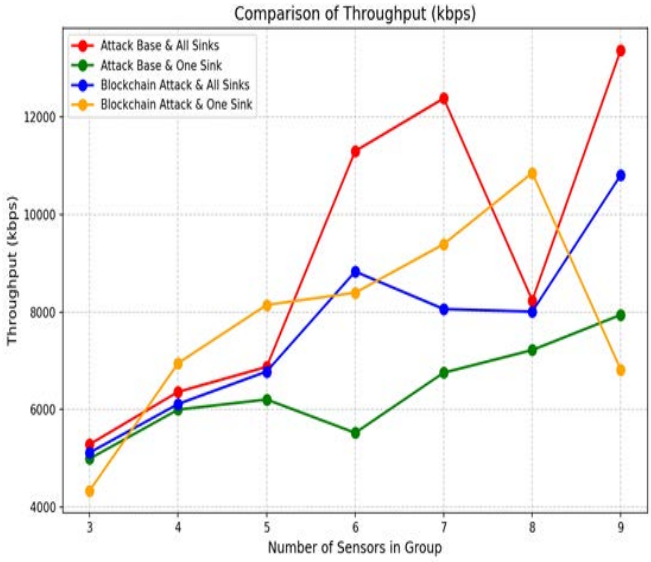


Figure 9: Impact of blockchain on throughput.

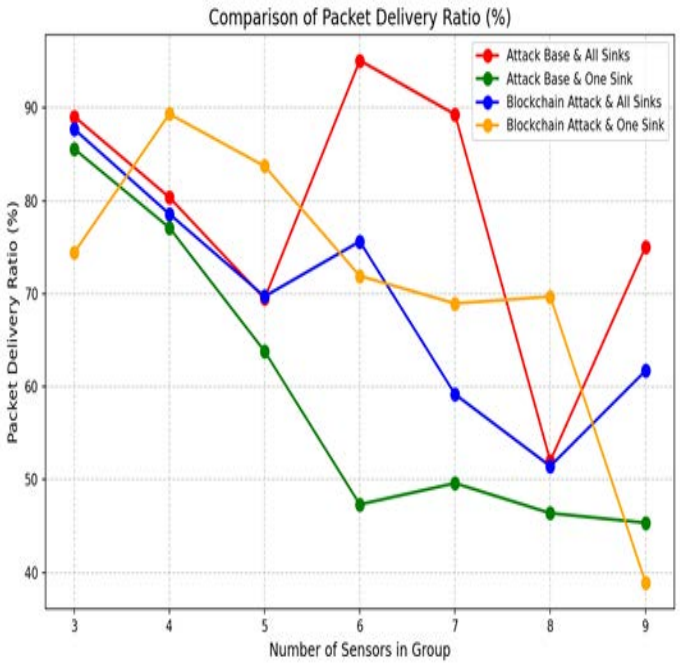


Figure 10: Impact of blockchain on packet delivery ratio.

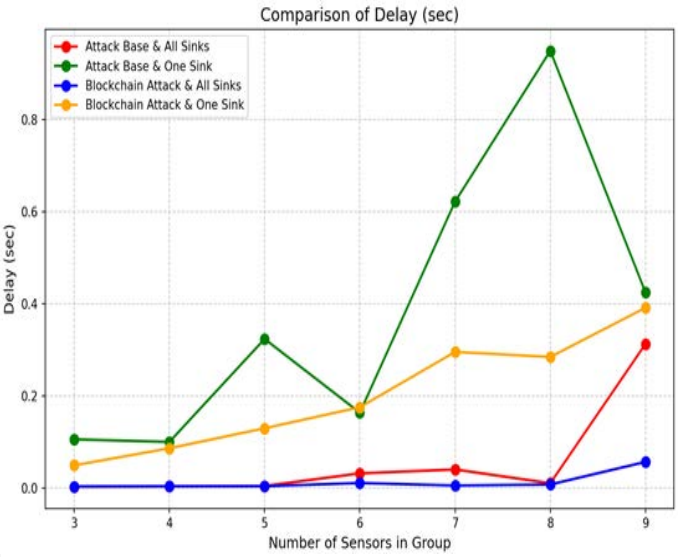


Figure 11: Impact of blockchain on packet delivery delay.

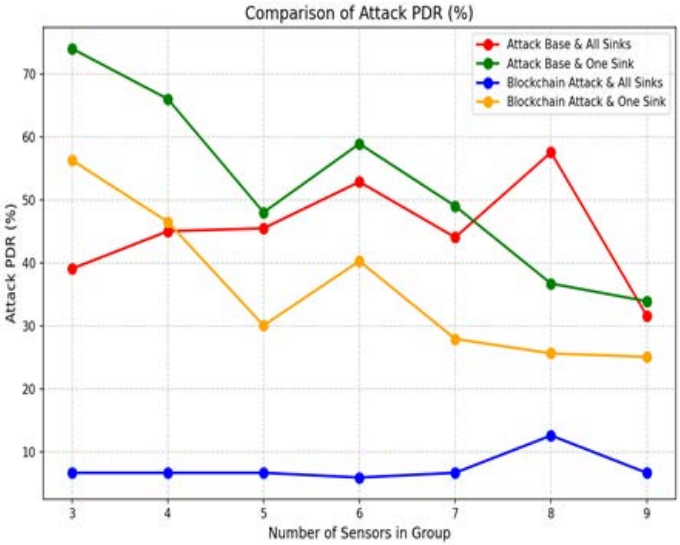


Figure 12: Impact of blockchain on malicious packet delivery.

Impact of SWDK Encryption

Distributed Attack Scenario: The deployment of SWDK encryption under distributed attack conditions resulted in a measurable throughput decline, ranging from 2% to 45.5% with a mean reduction of approximately 21%, relative to the unprotected state. A corresponding deterioration was observed in the Packet Delivery Ratio (PDR), which decreased by 8% to 45.8%. Latency behavior under SWDK was heterogeneous across the network. While most sensor nodes experienced reduced delays, counterintuitive improvements were recorded at specific nodes (3, 4, 5, and 9). Notably, the proportion of illegitimate packets delivered to the network interfaces declined dramatically, falling between 66% and 84%. Focused Attack Scenario: Under the concentrated attack model, the outcomes exhibited greater variability. Throughput improved across the majority of sensor configurations. The Packet Delivery Ratio (PDR) demonstrated significant improvement, with gains ranging from 21% to 44%. A and pronounced latency reduction—between 65% and 90%—was also observed. Moreover, the reception rate of illegitimate packets was curtailed by 19% to 47%. Implementing encryption resulted in an additional operational overhead caused by the increase in packet size following the addition of the encryption key leading to a 21% reduction in throughput compared to the unencrypted scenario.

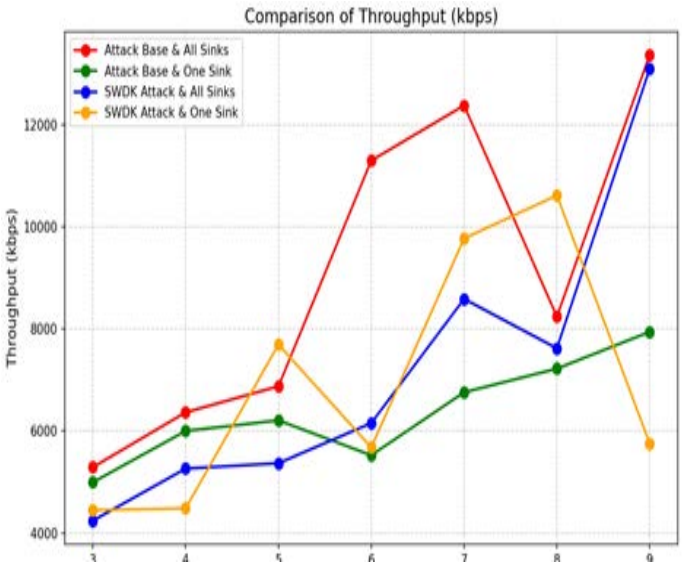


Figure 13: Effect of SWDK on throughput.

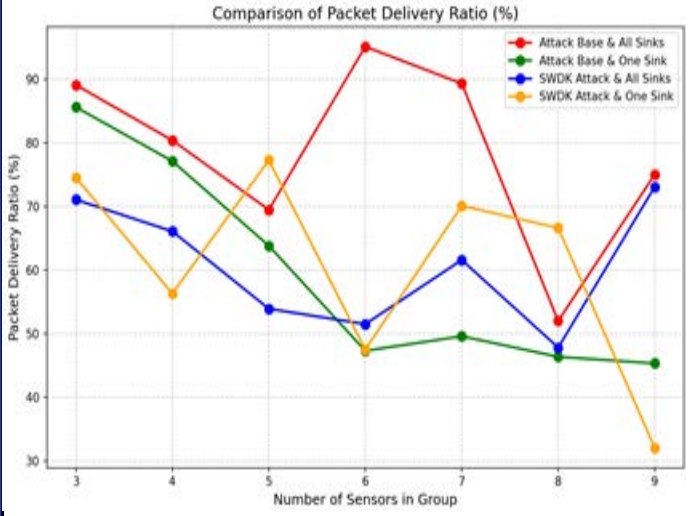


Figure 14: Effect of SWDK on packet delivery ratio.

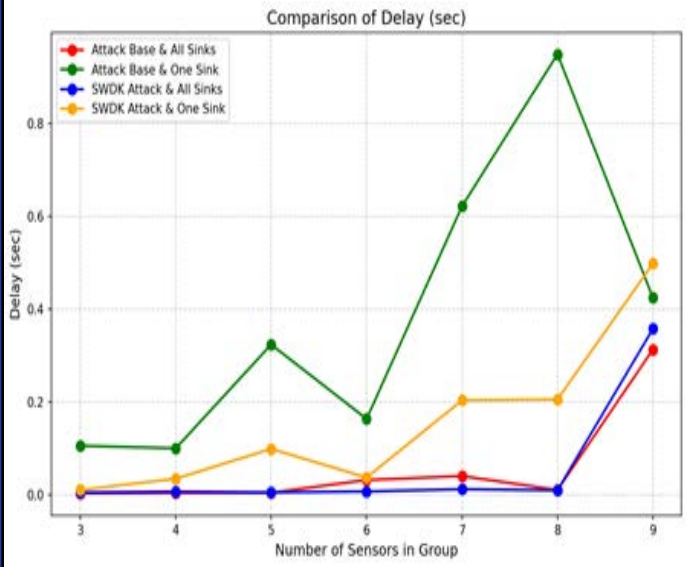


Figure 15: Effect of SWDK on packet delivery delay.

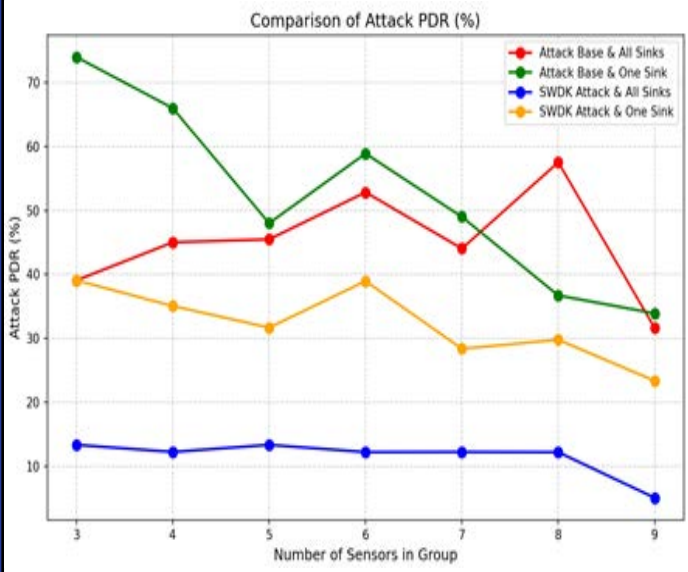


Figure 16: Effect of SWDK on malicious packet delivery.

Impact of the proposed model (Blockchain + PCA + SWDK)

Distributed Attack Scenario: In the context of distributed attacks, the proposed integrated framework fulfilled its core defensive mandate with exceptional efficacy. The overall attack success rate was curtailed by 73% to 85%, as the Attack_PDR declined precipitously from a concerning baseline of 31%–57% to a minimal residual level of actually 6%–14%. This substantial security enhancement was achieved alongside certain operational trade-offs: a mean throughput reduction of approximately 25% and a corresponding decline in the Packet Delivery Ratio (PDR). Latency outcomes exhibited great variability across scenarios; While some configurations recorded notable improvements, others experienced significant increases ranging from 83% to 92%. Focused Attack Scenario: Conversely, under the concentrated attack model, the integrated framework exhibited markedly improved performance. Through registered significant gains, and PDR demonstrated significant improvement with improvements ranging between 12% and 34%. Latency was reduced across all test cases by 55% to 82%, achieving an average latency reduction of approximately 70% in single-sink environments. The reduction in Attack_PDR ranged from 12% to 45% with an average of roughly 33%, as the metric shifted from a baseline of 34%–74% down to 23%–40%.

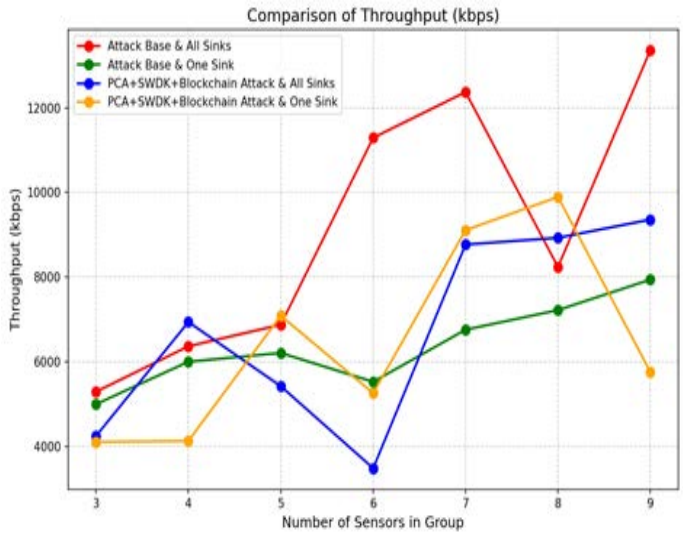


Figure 17: Impact of the proposed model on throughput.



Figure 18: Impact of the proposed model on packet delivery ratio.

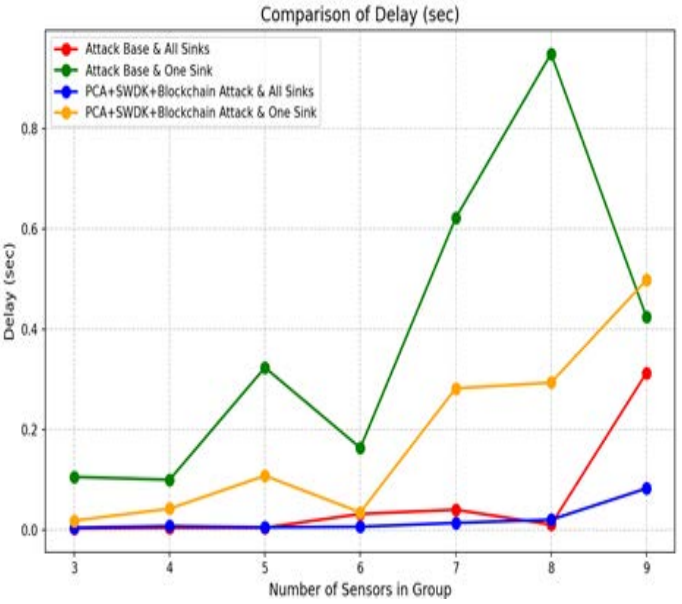


Figure 19: Impact of the proposed model on packet delivery delay.

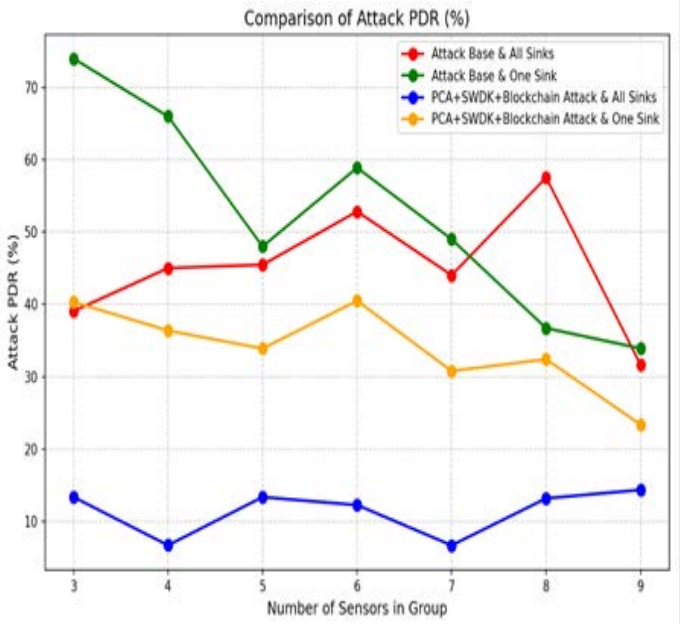


Figure 20: Impact of the proposed model on malicious packet delivery.

DISCUSSION

Blockchain

The blockchain layer, when deployed in isolation, demonstrated decisive performance against distributed attacks (malicious packet delivery <7%, accuracy >93%), which is consistent with the findings of Arachchige et al. [9]. However, it exhibited a notable shortcoming under concentrated attacks targeting a single sink node, permitting 25%–56% of malicious packets to pass through. This contrasts with the uniform traffic scenarios evaluated by Elumalai et al., who reported 97.4% accuracy and 2.1% false positives. Furthermore, the latency observed with blockchain alone reached approximately 0.3 seconds, compared to 61 ms reported by Elumalai et al., a discrepancy attributed to differences in the consensus mechanism (PBFT) and network scale. This observation supports the conclusions of Draz et al. [8] regarding the trade-off between computational cost and enhanced network adaptability.

SWDK

The SWDK encryption, which is derived from the geometry of a spiderweb, achieved a 66%–84% reduction in illegitimate packets, with a concurrent throughput reduction of 21%. This performance is comparable to the dynamic key system proposed by Mohamed Anwar & Pavalarajan [6]. SWDK excels in concentrated attack scenarios, improving the Packet Delivery Ratio (PDR) by 21%–44% and reducing latency by 65%–90%, primarily due to the rapid discarding of malicious packets and the alleviation of queue congestion—a dimension not highlighted by Shakor et al. [7]. Moreover, the unexpected latency reduction observed at specific nodes (3, 4, 5, and 9) is attributable to the prevention of retransmission for damaged packets.

Efficacy of the Integrated Hybrid Model (SWDK + PCA + Blockchain)

The complete model surpassed both its individual components and prior hybrid frameworks, as evidenced by the following: Attack Success Rate: Decreased by 73%–85% in distributed attacks, surpassing the detection rate of Jawahar et al. [5] (94% with 3.2% false positives). Latency Stability: Achieved an average reduction of ~70% in concentrated attacks, outperforming the 297 ms delay reported by Al Ebrahim et al. [2], while simultaneously achieving a lower malicious packet delivery rate (6%–14%). Trade-offs: Throughput decreased by 25%, which is consistent with the computational costs inherent in hybrid solutions such as those presented by Prasad et al. [10] (accuracy of 95.51%). However, the current model provides a more favorable and justifiable balance for sensitive applications, achieving a classification accuracy of 93%. Scalability: Multi-sink distributions demonstrated superior efficienviding quantitative

cy, effectively extending the principles of Rai et al. [11] for mitigating Denial-of-Service (DoS) attacks. The model exhibits performance fluctuations under high-density distributed attacks (latency increase of 83%–92%), attributed to the complex interplay between processing overhead, compression ratios, and queue management. This observation echoes the warnings of Abughazaleh et al. Concerning network saturation. Furthermore, the assumptions of static nodes and open-channel models constrain the generalizability of the results compared to dynamic or mobile environments (Halgamuge & Niyato [12]).

Comparison with Related Studies

In comparison with Reference [6], with which the present study shares a unified architectural philosophy, both approaches employ a Spider-Web-based Dynamic Key (SWDK) for lightweight encryption, Principal Component Analysis (PCA) for data compression, and a blockchain layer for tamper-resistant data aggregation. Both also adopt a two-stage security model—from sensor to aggregator and from aggregator to the base station—along with a category-aware encryption strategy that assigns varying key strengths according to data sensitivity. Nevertheless, the two studies diverge in several fundamental respects. First, whereas Reference [6] focuses primarily on reducing energy consumption, transmission cost, and storage cost within a 50×50 network simulated in MATLAB, the present study targets resilience against Denial-of-Service (DoS) and flooding attacks in an NS-3 environment, using a cluster-based topology comprising one base station and four sink nodes. Second, Reference [6] incorporates a routing mechanism based on neural networks optimized by the Bacterial Foraging Optimization (BFA) algorithm, while the proposed model relies on a private (permissioned) blockchain operating under a Proof-of-Authority (PoA) consensus mechanism, specifically tailored for cluster-based Wireless Sensor Networks (WSNs). Third, and most importantly, Reference [6] does not evaluate its scheme under adversarial attack scenarios, nor does it report attack-related metrics such as the Attack Packet Delivery Ratio (Attack_PDR) or the attack success rate. In contrast, the proposed model demonstrates a 66%–84% reduction in illegitimate packet delivery under distributed attacks, a 73%–85% reduction in the overall attack success rate, and an approximately 70% reduction in average latency under concentrated attacks, albeit accompanied by a trade-off of roughly 25% in throughput. Thus, the SWDK layer in the present study extends the findings of Reference [6] by shifting the evaluation from a purely performance-oriented assessment to a security-oriented, attack-aware one, providing quantitative evidence that SWDK is not only resource-efficient but also effective in countering DoS and flooding threats. Unlike the system in Reference [3]—which relied on a Proof-of-Authority (PoA) framework with a distributed detection mechanism, achieving high detection accuracy (exceeding 97%) and a latency of 61 ms, yet neglecting data compression—the proposed model integrates encryption to ensure security and data confidentiality alongside a compression algorithm to reduce data size prior to transmission. Furthermore, it employs blockchain technology to enhance reliability, mitigate flooding attacks, and detect malicious packets before they reach their targets. Consequently, this tripartite model successfully blocked attack packets at rates ranging from 73% to 85% in distributed attack scenarios (involving the base station and four sinks) and achieved a 70% response rate in concentrated attack scenarios (involving the base station and a single sink), albeit at the expense of a 25% reduction in throughput.

Table 1: Comparative summary of evaluated scenarios.

Scenario	Average Throughput (kbps)	Legitimate PDR (%)	Average Delay (s)	Attack_ PDR (%)	Security-Performance Balance	notice
No Protection (Under Attack)	7374–7741	56.00–66.31	0.0714–0.3934	48.00–60.28	None	—
Blockchain Only	8497–8787	69.50–73.49	0.0386–0.1770	3.79–44.00	Moderate	Best throughput (single-sink attack)
SWDK Encryption Only	7636–8354	64.00–71.85	0.0799–0.2180	8.75–38.50	Good	Balanced performance (single-sink attack)
Proposed Model	7157–7732	61.70–66.36	0.0380–0.1660	9.67–40.70	Excellent	

CONCLUSIONS AND RECOMMENDAIIONS

Based on what this study found, a few core recommendations are suggested to push the integrated framework further, especially in terms of performance, security, and scalability: First, the queue handling at the aggregation node needs to be upgraded by adding smarter scheduling algorithms. Such mechanisms are essential to prevent latency degradtion and even risk a sort of collapse once the active sensors get to around 5 or 6 nodes, which showed up as a critical turning point in the experiments. Second, adaptive compression is worth adopting, meaning the compression factor inside the Principal Component Analysis (PCA) approach should be adjustable on the fly. In practice, the compression ratio should rise automatically as the network gets close to its saturation zone, so congestion is reduced and communication reliability stays intact, even when traffic is heavy. Third, there's a clear point about accepting engineering trade-offs. A small drop in throughput might be allowed on purpose, if that leads to big improvements in detection accuracy and better temporal stability. Still, these trade-offs should be tuned carefully to match the needs of each particular use case, so you end up with a good equilibrium between security and performance, not just one side getting all the attention. Fourth, it is recommended to do periodic renewal of the spiderweb network parameters. This work should be handled through a secure protocol, so the confidentiality stays intact and robustness remains solid for the dynamic keys, and so you can avoid any likely key compromise over longer operational stretches. Finally, future work should concentrate on scaling up and hardware acceleration. It would be good to test the proposed system on larger scale network topologies, and also run it against a wider spectrum of attack types. In addition, doing a hardware level implementation of the SWDK encryption layer is encouraged, to sharply cut down computational overhead, which in turn should improve overall efficiency and responsiveness when you deploy it in real-world situations.

REFERENCES

1. Demirci S, et al. Depth-First Search-Based Malicious Node Detection with Honeypot Technology in Wireless Sensor Networks. Mathematics. 2026;14(6):1050.

2. Al Ebrahim A, Badawieh A. Machine Learning-Based Detection and Prevention of DoS and DDoS Attacks in SDWSN. Iraqi Journal for Electrical and Electronic Engineering. 2026;22(1):114-127.

3. Vailshery LS. Global IoT and Non-IoT connections 2010–2025 [Internet]. Statista; 2021 [cited 2026 Aug 23]. Available from: https://www.statista.com/statistics/1101442/iot-number-of-connected-devicesworldwide/.

4. Elumalai G, et al. A blockchain-driven intrusion detection model for secure communication in IoT-WSN mesh architectures. Peer-to-Peer Networking and Applications. 2026;19(2):60.

5. Jawahar A, et al. DDoS mitigation using blockchain and machine learning techniques. Multimedia Tools and Applications. 2024;83(21):60265-60278.

6. Mohamed Anwar A, Pavalarajan S. Spider web-based dynamic key for secured transmission and data-aware blockchain encryption for the Internet of things. IETE Journal of Research. 2024;70(1):499-514.

7. Shakor MY, et al. Dynamic AES encryption and blockchain key management: a novel solution for cloud data security. IEEE Access. 2024; 12:26334-26343

8. Draz U, et al. Decentralized energy swapping for sustainable wireless sensor networks using blockchain technology. Mathematics. 2025;13(3):395.

9. Arachchige KG, et al. Blockchain-enabled mitigation strategies for distributed denial of service attacks in IoT sensor networks: An experimental approach. Computers, Materials & Continua. 2024;81(3):3679-3705.

10. Prasad A, Arockiasamy K, Gunasekaran K. A hybrid metaheuristic algorithm with machine learning for detecting denial-of-service attacks in wireless sensor networks. Frontiers in Artificial Intelligence. 2026; 9:1738152.

11. Rai HM, et al. Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. Heliyon. 2024;10(19): e38100.

12. Halgamuge MN, Niyato D. Adaptive edge security framework for dynamic IoT security policies in diverse environments. Computers & Security. 2025; 148:104128.

13. Saheed YK, Abdulganiyu OH, Ait Tchakoucht T. Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities. Applied Soft Computing. 2024; 155:111434.

14. Abughazaleh N, et al. DoS attacks in IoT systems and proposed solutions. International Journal of Computer Applications. 2020;176(33):16-19.

15. Ren B, et al. A multiagent deep reinforcement learning autonomous security management approach for Internet of Things. IEEE Internet of Things Journal. 2024;11(15):25600-25612.

Author contributions

Conceptualization: Razan Rezk

Methodology: Razan Rezk

Investigation: Razan Rezk – Dr. Wasim Al-Juneidi

Project Administration: Razan Rezk

Supervision: Dr. Wasim Al-Juneidi

Writing – Original Draft: Razan Rezk

Writing – Review & Editing: Razan Rezk – Dr. Wasim Al-Juneidi

Competing interests: No conflict of interest exists.

Data and materials availability: All data are available within the main text and supplementary materials

Abbreviations

abbreviation	Expression
IoT	Internet of Things
WSN	Wireless Sensor Network
WSNs	Wireless Sensor Networks
DoS/DDoS	Denial of Service / Distributed Denial of Service
SWDK	Spider Web Dynamic Key
SWC	Spider Web Construction
PCA	Principal Component Analysis
PDR	Packet Delivery Ratio
Legitimate PDR	Legitimate Packet Delivery Ratio
Attack PDR	Attack Packet Delivery Ratio
NS-3 / ns3	Network Simulator 3
QoS	Quality of Service
SDWSN	Software-Defined Wireless Sensor Network
TDFS	Tree-based Depth-First Search
ML	Machine Learning
GOA	Grasshopper Optimization Algorithm
GA	Genetic Algorithm
MLP	Multilayer Perceptron
KNN	K-Nearest Neighbors
CART	Classification and Regression Trees
LR	Logistic Regression
GRU	Gated Recurrent Unit
PBFT	Practical Byzantine Fault Tolerance
SVM	Support Vector Machine
AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
PoS	Proof-of-Stake