Received: 17 July 2023 | Revised: 22 May 2024 | Accepted: 20 July 2024

DOI: 10.1002/spy2.450

SURVEY ARTICLE

WILEY

A deep experimental analysis of energy-proficient firewall policies and security practices for resource limited wireless networks

S. Rajasoundaran[1] | **S. A. Sivakumar**[2] | **S. Devaraju**[3] | **M. Jahir Pasha**[4] | **Jaime Lloret**[5]

[1]Department of Computer Science, Samarkand International University of Technology, Samarkand, Uzbekistan

[2]Department of Electronics and Communication Engineering & Dean-Academics, Ashoka Women's Engineering College, Kurnool, India

[3]School of Computing Science and Engineering (SCSE), VIT Bhopal University, Sehore, India

[4]Department of Computer Science and Engineering (Data Science), Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, India

[5]Instituto de Investigacion para la Gestion Integrada de Zonas Costeras, Universitat Politecnica de Valencia, Valencia, Spain

Correspondence
Jaime Lloret, Instituto de Investigacion para la Gestion Integrada de Zonas Costeras, Universitat Politecnica de Valencia, C/Paranimf, 1, 46730 Grao de Gandia, Valencia, Spain.
Email: jlloret@dcom.upv.es

Abstract

The role of firewalls and security principles in resource-limited wireless networks and Wireless Sensor Networks (WSN) is more expected than in any dedicated network environment. The advanced wireless technologies and emerging fashion of autonomous wireless network nodes are mostly expecting resilient firewall services with multi-level security policies. Wireless networks are classified under sensor networks, Internet of Things (IoT) mobile networks, and so forth. According to the expectations, security frameworks are gradually invented around the communication platform using various ideologies. The novel ideology and respective implementation effort open better solutions against wireless network attacks. Anyhow, the minimal production of time complexity, energy complexity, and computation overhead from any novel security approach is always considered under the best practices. The complexity levels directly affect the wireless node's energy consumption ability and operational spans severely. The energy optimization techniques and load-balancing techniques integrated into multi-class firewall rules are extremely useful solutions for resource-limited wireless networks. This article has been motivated to analyze the recent firewall techniques and secure data communication mechanisms used for securing wireless networks. Consequently, the practice of comparative literature analysis helps to improve the current limitations identified under the classified categories of security mechanisms such as energy-optimized security principles and load-balanced security principles. The establishment of secure and energy-optimized multi-class firewall rules in each wireless node assures a healthy focus on next-generation networks. The experiment section shows the benefits of energy-optimized secure network communication in terms of better accuracy and the benefits of load-balanced secure network communication through minimal overhead in computing platforms.

KEYWORDS

attacks, artificial intelligence, energy efficiency, firewall, internet of things, security, wireless networks, wireless sensor networks

1 | INTRODUCTION

Firewalls are the devices deployed in the network to enable secure data traffic between the organization network and the outsider network. The security policies established for protecting the network from threats and attacks are implemented according to particular organization rules. Network security is intended to secure data traffic management policies that are changing based on the deployment strategies of various platforms.[1,2] According to the type of network architecture and operation models, a suitable type of firewall is required.

The types of firewalls consist of packet filtering firewalls (static, reactive, stateless, and stateful), proxy firewalls or application firewalls, stateful inspection firewalls, circuit-level firewalls, next-generation or future-generation firewalls, and unified threat assessment firewalls. The selection of a particular firewall model is an important practice concerning demand-based security expectations. The security model of each organization is expected to be secured using either protocols' hardware firewall units or software firewall units. Generally, packet filtering firewalls and circuit-level firewalls are used to capture and analyze the Internet Protocol (IP) address and service port number in each data packet crossing the firewall. The basic firewall model is used to manage the security policies using these socket verification rules. These models are simple to configure yet not efficient to analyze other internals of data packets.[3,4] Also, this type of firewall does not manage the entity details or states.

The recent development of firewall policies allows the improvement in packet filtering firewall systems with state management and reactive decision systems. Proxy firewall or application layer firewall policies are configured to analyze the website services, Hypertext Transfer Protocol (HTTP) requests, web responses, packet contents, and application requests. In addition, the proxy firewall acts as an original system to lure outsiders and protects the identity of web systems. In contrast, a proxy firewall takes more time to analyze the packets and consumes more energy compared to a packet-filtering firewall and a circuit-level firewall. Likewise, the policies used for implementing proxy firewalls are not suitable for all network protocols (data formats).

A stateful inspection firewall is the most useful component for tracking network events and malicious data based on established sessions. It gives more crucial security benefits than other firewall designs yet the increasing load due to tracked records causes moderate network performance. Next-generation firewalls and unified threat assessment firewalls are executing deep data extraction policies with the help of suitable security algorithms. These firewalls analyze the packet header and payloads through HTTP transactions. The efficient and complex nature of these firewall designs leads to costly deployment issues. In addition to that, various models of software-defined firewalls, Artificial Intelligence (AI) based firewalls, cloud firewalls, Network Address Translation (NAT) firewalls, and other research-based firewalls are proposed to secure the network.[5]

Mostly, firewalls are generalized as software-assisted hardware units to build a strong security perimeter rather than choosing fully software units. Anyhow, optimal energy consumption and computation management policies are necessary to design a new type of firewall system under feasible network applications. In this connection, the energy optimization quality can be achieved through properly designed firewall computation rules and security practices. Current firewall models suggest feasible security solutions and firewall principles against network anomalies. According to the deep analysis of security considerations, this article finds the real-time problems of a growing population of network devices around the world. The continuous improvement of network communication technologies requires different types of terminal devices and connecting units. In this regard, various industries expect application-based network models in public and private environments. These networks are expected to operate under protected circumstances.

On this basis, anomaly detection rules and attack detection practices are created in the firewall system. The ruleset for various types of firewalls is created against a particular type of attack. Anyhow, the limitations of the firewall ruleset affect the overall security practices. The best security practices of complex firewall systems are analyzed by various researchers. The earlier work discusses the benefit of creating optimal use of secure healthcare networks. Similarly, the later work identifies the importance of uniform traffic distribution for managing firewall workload optimally. Secure healthcare systems have been created to protect radio communications, medical data-sharing policies, and user management systems. Secure firewall policies are practiced against attacks such as Denial of Service (DoS), website injections, data eavesdropping, malware, reconnaissance, and other worms. Under this condition, this work states the importance of the firewall rules for the packet filtering model, web-based packet analysis model, cloud monitoring model, next-generation model, and other security models. Additionally, the networks are suffered due to improper handling of communication overhead. Against the load distribution problems and firewall activation problems, the need for well-defined and lightweight multi-firewall security policies is widely expected.

The expectation of multi-class firewall policies and secure private firewall models are crucially playing among research groups. Al-Haija et al.[6] propose multi-class firewall rules for monitoring web traffic using suitable classification models. The neural classification model analyzes the incoming packet attributes using appropriate training phases. The firewall system is trained with the help of the web firewall dataset (2019). This dataset contains both legitimate and malicious events regarding web traffic. The firewall analyzes and allows legitimate packets based on a trained neural system. The classifiers of the firewall are configured for stating the conditions of "packet allow," "packet block," and "reset." In the same manner, Rahman et al.[7] introduced software-assisted cybersecurity techniques using deep learning mechanisms. Particularly, deep learning mechanisms are applied to improve the efficiency of future-generation wireless communication security environments. The motivation of this technique is to focus on intelligent attacker communities. Additionally, the perspective of the industrial Internet of Things system helps to improve the heterogeneous network security principles.

From these articles, we can understand the currently implemented cyber security models, firewall principles, and energy-efficient attack monitoring schemes among both wireless networks and wired networks. The related articles used for the technical analysis of energy-optimized firewall security principles contain crucial security aspects. The security aspects discussed in this article are listed as firewalls and security benefits in wireless networks, security circumstances and energy optimization policies, and notable aspects of security practices and load-balancing techniques.

1.1 | Motivation and contribution

From the given aspects, this experimental analysis has been motivated to analyze existing security techniques and firewall policies against various performance metrics. The existing research works mainly focus on energy optimization strategies for securing the network perimeters. The main challenges in finding suitable energy-optimized security (firewall) principles are lack of accuracy, urea liable device-based procedures, failure in resource estimations, and load-sharing failures in distributed networks. In the stream, the existing survey works ignore load-balanced security techniques, and resource-sensitive security policies with clarity to prove the stability of security solutions. This is considered a major research problem in this article. On the technical scope, this article contributes to the development of future-ready security principles for wireless networks. The significant contributions of this survey are listed below. Analyzes the technical benefits and limitations of energy-sensitive security policies suits for distributed networks.

- Discusses the theoretical and experimental opportunities of load-balanced security policies suitable for lightweight networks.
- Understands and identifies the merits and demerits of resource-limited security solutions suitable for wireless networks.
- Suggests optimal solutions to build effective firewall/security algorithms for resource-limited wireless networks.

Specifically, the proposed research extends its contribution to analyzing the security solutions for wireless networks with limited resources. The research article has notable assumptions on related works as follows for suggesting the optimized energy-efficient firewall/security policies.

- Networks that are modeled for hostile and outdoor environments.
- Networks with limited battery charging capabilities.
- Networks that are modeled for specific applications with limited memory and processor resources.
- Edge-connected and cloud-connected wireless nodes.
- Wireless networks that are modeled for distributed and lightweight intrusion detection procedures (Not centralized).
- Networks that run with multi-point firewall monitoring procedures.

Based on the assumptions, the survey has been conducted on reliable security procedures to ensure minimal consumption of network resources. On the scope, the security procedures make possible solutions through load-balanced firewall policies, security policies with energy-optimization solutions, lightweight distributed firewall mechanisms, and reliable intrusion detection systems. By the way, the article is organized through various sections. Section 2 of this article

describes research materials collected for expressing the technical contributions of various firewall-based security mechanisms. Section 3 illustrates the experimental setups and implementation details. Section 4 concludes the article with identifications, limitations, and future directions.

2 | MATERIALS AND METHODS

Security mindset and continuous practices against various cyber-attacks are essential needs for any network. The security policies are defined against attacks and malicious behaviors using software-defined rules and hardware devices. The deployment of hardware devices and software applications to monitor the attacks may vary from one type of network to another type of network. Diansyah et al.[8] propose an experimental analysis of firewall utilization and a centralized honeypot model for organizing a secure wireless network. The combination of both firewall and honeypot policies against various attacks. The firewall rules are configured to control access to internal network assets (allow or deny). In addition, this work implements single honeypot rules for creating traps against attacks.

The integration of firewall-blocking policies and honeypot trap models creates better security solutions. Both systems coordinate with each other to control the attacks coming into a real wireless network environment. In the model, the experimental setup provided an open-source honeypot platform (Honeyd) for analyzing the network traffic. Honeyd platform has low interaction services for file transactions, secure shell interactions, and web protocol. In the testbed, Honeyd firewall policies are developed with real server units, honeypot server units, and client interactions. Among the client interactions, the Honeyd-based firewall setup identifies legitimate requests and malicious requests raised via applications. The observations of this experiment revealed the extraction of vulnerable ports and protocol addresses. Anyhow, this system justifies the complexities of finding open-channel attackers.

In this regard, Srinivasavarma et al.[9] analyze the principles of network intrusion detection systems and hardware-based packet classification policies. In addition, this work observes the existing multi-objective packet classification rules and packet header analysis policies. In the same way, this scheme has been equipped with data compression techniques and packet structural properties for improving network security. As this is a hardware-based packet classification mechanism, the security policies and packet classification policies are implemented in the network computational unit. The article has experimented this multi-level packet classification rules using ternary content addressable memory cells. These cells are designed and built on a hardware platform with bit-wise operators. These bit-wise operators collect the packet information in binary format and initiate multi-level packet classification rules. The hardware-based multi-level ternary content addressable memory cells work with a priority encoder module to find the best classification (high) results via pre-programmed rules. The article states that hardware-based programmable arrays and memory cells mainly provide faster execution of packet classification procedures compared to software-based rules. In contrast, this method is not flexible for customization rules.

Similarly, next-generation security models and firewall implementation strategies are focused on green energy management schemes and lightweight firewall engines. As communication technology emerges towards high-interaction data platforms and tiny device deployment strategies, the need for optimal energy-saving plans is mandatory at any cost. In this manner, Zhang[10] and Akin et al.[11] are discussing next-generation security models and firewall rules. Notably, the earlier work contributed to future-focused security designs and firewall deployment plans for managing hospital database systems. Both articles created an experiment based on virtual network groups to build security policies. In Reference 10, virtual LANs hold the distributed firewall policies against various attacks (identity attacks, integrity attacks, confidentiality attacks, etc.). The simulation conducted in this experiment utilized virtual network-based dynamic internet protocol addresses and independent firewall rules for protecting different sets of medical data. This work justified that the heterogeneous firewall policies and distributed network conditions guard medical data against crucial attacks. In the same manner, Reference 11 proposed fifth-generation energy-efficient security policies using network slicing functions. In the experiment, network slicing functions have been initiated with different network parameters (differentiated services). The firewall-based security policies of this network slice are experimented with under different sets of latency, throughput, virtual connections, physical connections, server configurations, and client configurations. This work justifies the experimental security analysis for several server nodes with supporting client nodes.

Nowadays, healthcare management systems are widely utilizing computerized resources to maintain patient data, health records, and other real-world data. This work initiates the security practices and plans for building efficient firewall models for local area networks and virtual private circumstances. According to that, the later work builds energy-efficient software-defined networks with optimized network slicing practices. In this work, the network management policies are

taken using various levels of quality metrics. This practice helps to minimize energy wastage in the network security principles. The research practices on energy-efficient firewall establishment policies are growing around the world to ensure the security of heterogeneous platforms. Yi et al.[12] identify the security issues in wireless sensor networks and propose green firewall policies to protect the distributed sensor nodes. In this concern, the main constraint noted in the Wireless Sensor Network (WSN) is the resource limitations of sensor nodes. The mandatory solution against intrusions and attacks over sensor nodes must be addressed through lightweight packet analysis mechanisms. The practice of energy-optimized attack detection and isolation rules is deeply analyzed in this scheme. The experimental study of this work observed the detection of attacks effectively and produced a limited rate of intrusion alarm. The experiment was specifically conducted to analyze power-efficient security mechanisms for WSNs. The testbed created in this work has 300 sensor nodes and "n" attackers that can inject both active and passive attacks.

A green firewall in each sensor node is initiated for detecting intrusions under distributed architecture. The firewall's performance was significant in WSNs, still, these procedures were not suitable for other types of networks.

Schwarz[13] provide a detailed analysis of the security aspects related to operating system services, data traffic collected from network interface cards, trusted gateway points, code execution services, remote accesses, and other activities happening in the network. In addition, this work finds the trusted gateway-based firewall configuration rules against external attackers. Generally, gateways are considered for improved security features between internal and external networks. In this regard, circuit-level gateway firewall policies improve the security benefits of the network. Additionally, the trust rate between various services and resource-sharing events must be highly expected under surveillance to detect malicious events. These qualities of a secure network ensure the protection of stable data in the network. At the same time, data on the channel must be secured through trusted routing policies. The trusted routing policies between adjacent nodes need to be configured to ensure secure multi-hop routing on the channel. Anyhow, the energy spent for each session is counted as a major resource metric. The developed test base of a trusted execution environment contained trusted gateways with ARM security policies and traffic validation factors. These test bed experiments accommodated various suspicious actions like malfunction attacks, gateway-breach attacks, and interface attacks (ports). In this condition, the developed ARM trust network ensured the differentiated firewall policies against different attacks. Through these policies, the trusted mechanism stabilized the secured throughput rate and legitimate network transactions. At the same time, the trusted policies were not customized to meet unknown malicious attacks that cause insecurity in the network.

On this basis, a detailed survey has been conducted by various researchers.[14] Specifically, the survey on energy-efficient firewall principles and procedures focused at various levels such as gateways, routers, servers, and internal distributed points. The focus of energy optimization techniques for firewall functions varies depending on the types of networks, architecture, resource availability, and the required rate of incident response against the attacks. According to the needs, the firewall policies can be designed under node-centric or network-centric rules.

ElSawy et al.[15] propose geographically distributed spatial firewall systems in outsized wireless networks. Large-scale distributed networks commonly expect multi-point security perimeters to identify region-based attacks. Particularly, wireless distributed networks with a large number of communication devices require specific region-based security policies to detect the attacks. In this concern, this work initiates distributed malware quarantine policies using randomly distributed firewall nodes. The spatial firewall nodes denoted in this mechanism are considered as the set of nodes around different regions of the network. These are called spatial firewalls. The spatial firewall nodes are randomly selected for monitoring and controlling the internal accesses and external traffic into the wireless network. In this case, the affected nodes, compromised nodes, or other infected servicing points are isolated to protect the network. On the scope, the distributed wireless network has been secured using spatial firewall rules which are lightweight and power efficient due to the nature of load distribution strategies. The implementation of spatial firewall policies includes the Internet of Things (IoT)/elements under distributed Cyber Physical Systems (CPS). In this case, distributed firewall nodes with rule bases are created among IoT/CPS units. These nodes communicate in this heterogeneous network through spatially distributed firewalls. The implementation setup has different rule-based firewall functions at various firewall nodes that help to improve the security and energy utilization rate in the network. At the same time, the spatial firewalls are limited in terms of handling bulk traffic and complex attacks.

In this fashion, Uçtu et al.[16] investigate the development of next-generation firewall systems with bridge-level configurations. According to the development strategies of future firewall models, newly expected attacks and unknown activities are seriously observed. The continuous observations and security practices are highly helpful to develop protected link layer and internet layer policies. The testbed conducts firewall-based intrusion detection practices in layer 2 (bridge mode-multicast network) and layer 3 (meeting point mode). The multicast group with different sets of nodes enables communication through group internet address. On this basis, firewall rules are computed and deployed to allow/block

the traffic at bridge points. In this case, bridge points are created to connect different multicast groups. The development of bridge-based firewall policies is highly useful in multicast communication, yet the internal nodes shall be validated for suspicious actions.

Guo et al.[17] develop energy-sensitive cyber security models for hybrid electrical vehicles. The autonomous electrical vehicular network is vulnerable to various types of attacks. Notably, attackers can easily affect the energy savings of each vehicular node. Over this problem, this work finds the distributed probability models against physical problems created by attackers and power wastages. In the vehicular system, the attackers create malfunctions using wireless channel attacks, sensor attacks, vehicular parameter attacks, and controller attacks. These attacks are initiated at different levels of vehicular cyber systems to harm power sources and controller units. The experiment has been conducted using energy management algorithms, and anomaly detection algorithms in vehicle units. In specific, the testbed monitors driving cycles (sensor data, parameters, controller function points, and wireless channel interference), and detects suspicious driving issues. In this case, this work identifies an overall stealthy probability rate against attacks and ensures secure driving practices.

In the same manner, Bagheri and Shameli-Sendi[18] manage the network security principles using dynamic and optimal firewall rules for detecting random attacks. In this process, optimization algorithms are developed for regularizing the multi-level ruleset of dynamic firewall models. This work clarifies the benefit of using multi-level dynamic rulesets to provide better solutions in terms of security breaches. The multi-level firewall systems consider the network parameters such as scalability, bandwidth, network slicing rules, and optimal firewall rule ordering procedures, among virtually implemented network regions. The experimental setup has packet-filtering firewall rules in the cloud model. The packet filtering firewall rules include the preprocessing phase of the ruleset, dependency identification, rule merger/splitter, firewall performance optimization, and rule weight analysis. These procedures are implemented in the cloud-based packet filtering firewalls for monitoring the attacks in need. In the cloud model, clients, servers, cloud routers, and supporting web services are deployed to create a realistic testbed against attacks. The observations of this experiment conclude that the multi-level cloud-based firewall rules perform effectively with a specifically developed heterogeneous rules set. Likewise, various types of firewall policies are emerging for providing energy-efficient security solutions, content-based security solutions, and load-controlled security solutions.[19-21] Table 1 shows the comparative solutions and limitations of various security methodologies discussed above.

From this literature discussion, the observations are gathered for future development models such as future-generation firewall solutions for wireless networks, energy-efficient firewall rules and security solutions, multi-level dynamic firewall principles, and intelligent distributed firewall systems. Apart from the discussions related to intrusion detection systems and secure routing principles, the assurance of minimum energy wastage is inevitable.[22-24] In addition, the heterogeneity of various network architectures (wired networks, wireless networks, centralized security points, distributed security services, dynamic network configuration aspects, etc.) and network properties are taken under serious consideration for next-generation energy optimization rules for implementing successful firewall systems.[25-27] In addition, the recent research articles identified the stream of resource-limited security policies are discussed in Section 3. As the survey finds the experimental discussions of resource-limited security algorithms (firewalls) are inevitable to locate the suitable monitoring points. In the concern, the resource-limited security mechanisms proposed recently find the distributed, centralized, and router-based firewall points to secure the networks.

3 | EXPERIMENTAL OBSERVATIONS, RESULTS, AND COMPARATIVE DISCUSSIONS

The article has concentrated on pointing out more variants of security models provided by research communities.[28,29] Especially, distributed networks, wireless network participants, heterogeneous network models, and lightweight network environments (resource-limited) are continuously expecting energy-controlled firewall security procedures. As illustrated in Table 2, Durante et al.[3] proposed multi-level firewall implementation policies for examining the packets with a minimal single-point load (Figure 1). In this regard, the test bed of the multi-layered firewall system has been configured between the appropriate source and destination.

As discussed in previous sections, many researchers have contributed to energy-optimized security protocols and firewall policies (Table 3). The performance on the simulation testbed between different techniques is evaluated using metrics such as average energy consumption rate (Joule), secure packet delivery rate (kbps), event detection delay (milliseconds), computation overhead (%), system accuracy rate (%), false positive rate (%), and system error rate (%). These

TABLE 1 Literatures—energy optimization policies and security policies.

No.	Articles	Methodologies	Solutions and research problems	Limitations
1	Diansyah et al.[8]	Integrated security policies of honeypot systems and centralized firewall rule engines.	Dual Security solutions against real-time malicious events.	The lack of coordination between the honeypot and firewall leads to functional problems.
2	Arif et al.	LSTM-based trained network routines to optimize the Quality Of Service (QoS) metrics (delay, bandwidth, throughput, energy, and load).	QoS data analysis schemes and machine learning frameworks for security issues among mobile edge nodes.	Energy consumption due to deep LSTM networks shall be minimized in lightweight mobile edge circumstances.
3	Srinivasavarma et al.[9]	Hardware platform manipulations and changes to implement multi-classifier rules with energy optimization policies.	Energy-optimized hardware solutions against NIDS issues and real-time packet classification issues.	Lack of flexibility and scalability for future modifications.
4	Zhang[10]	A study on healthcare data security solutions with future generation firewall policies.	Field-specific discussions and research aspects are extracted against malicious activities.	Targets only medical-based data security models no other critical networks.
5	Akin et al.[11]	Software-defined networking functions with virtual network monitoring solutions based on QoS metrics.	Network slicing methods through green computing approach to reduce energy consumption rate.	Nonlinear dynamic secure programming strategies are not used for security frameworks but linear solutions.
6	Yi et al.[12]	Establishment of secure wireless sensor networks by deploying energy-efficient and distributed attack prevention mechanisms.	Lightly loaded Security principles are initiated for tiny sensor nodes against intrusions.	Firewall has limited classification strength for extracting attack features.
7	Schwarz[13]	Trusted circuit-level gateway firewall policies are deployed and distributed trust zones are created for secure routing paths.	It is a better solution with secure routing and firewall monitoring policies against multiple attacks.	Computations of dynamic trust levels are complex in real-time environments.
8	Chauhan et al.[14]	A study on energy-optimized security services for smart network environment.	Informative solutions and objectives are provided from vast discussions.	Need appropriate experimental testbeds.
9	ElSawy et al.[15]	A unique idea of building spatially distributed firewall policies that are implemented in multiple wireless nodes.	It is providing lightweight security solutions and geographically distributed firewall activities against attacks.	All are resource-limited nodes and they are not evaluated energy abnormality cases.
10	Uçtu et al.[16]	Multicast network communication and threat prevention principles for future firewall models.	Group security solutions against network attacks.	Multiple threats and attacks are not analyzed in detail.

TABLE 2 Multi-set rules and packet field analysis.

Rules	Packet field-1 (bit positions)	Packet field-2 (bit positions)	Packet field-3 (bit positions)
R1	B1	B2	B3
R2	B4	B5	B6
R3	B7	B8	B9
R4	B10	B11	B12
R5	B13	B14	B15

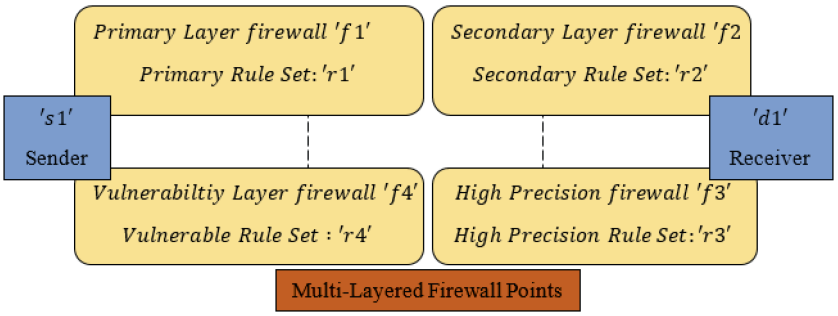

FIGURE 1 Multi-layered firewall policies.

TABLE 3 Firewalls with energy optimization strategies.

No.	Articles	Experimental features	Load distribution strategy	Energy optimization strategy
C1	Durante et al.[3]	Multi-level firewall configuration policies and traffic load distribution schemes.	✓	
C2	Rahman et al.[6]	Industrial IoT systems and sixth-generation network security policies using deep learning-based software-defined secure networks.	✓	
C3	Arif et al.	Minimizing the energy consumption rate through controlled overload using LSTM networks in mobile edge networks.		✓
C4	Srinivasavarma et al.[9]	Hardware model development for multi-data classification rules and energy control.		✓
C5	Yi et al.[12]	Energy controlling mechanisms to enable distributed security policies in wireless sensor networks.		✓
C6	ElSawy et al.[15]	Identifying and Isolating malware attacks in large community wireless networks.	✓	
C7	Radhakrishnan et al.[19]	Cyber physical systems for monitoring energy loss and context-sensitive plug load issues.		✓
C8	Demirci and Sağıroğlu[28]	Security management policies through software-defined network principles and virtual security principles. In addition, this scheme achieves energy efficient routing tasks.		✓
C9	Kumar et al.[33]	Underwater security management and lightweight firewall implementation strategies.		✓
C10	Khanum et al.[35]	Real-time energy sensitive solutions for implementing sensor-based intrusion detection systems.		✓

TABLE 4 Simulation parameters and implementation details.

No.	Network configuration metrics	Measurements
1	Number of wireless nodes	500
2	Initial energy (J)	60
3	Transmission energy (J)	3.45
4	Receiving energy (J)	1.98
5	Geographical area (m^2)	1000
6	Channel bandwidth	30 kHz
7	Channel frequency	2.4 GHz
8	Channel throughput	100 kbps
9	Signal propagation	Two-Ray Ground/Omnidirectional
10	Simulation time/iterations	200 s/20
11	Routing protocol	AODV
12	Bit rate	Variable
13	Tools	Network Simulator 3.35

performance parameters are closely related to analyzing the testbed behaviors of security mechanisms imposed through either load-balancing strategies or energy optimization strategies. As mentioned in Table 4, this experimental study has been evaluated under the NS-3.35 testbed (C++ and Python libraries). As the related energy optimization techniques are taken from various platforms, the experimental conditions of this work have been set for nominal and common network configurations as given in Table 4. In this regard, the wireless network has been configured with a maximum range of 500 nodes around 1000 (m^2) field. The frequency limits and channel bandwidth configurations are set as nominal values for compared works in the simulator environment.

As mentioned, the existing security techniques and firewall models are categorized under unique energy optimization strategies and traffic load-balancing strategies.[30-32] Both types of techniques ensure a crucial impact in each wireless node to normalize or reduce the energy utilization in the network.[33,34] On this scope, this study has found three recent balanced security mechanisms[3,6,15] and seven energy-optimized security mechanisms[9,12,19,28,33,35] to evaluate the security achievements in need. The detailed discussion of energy-optimized security mechanisms and load-balanced-security mechanisms helps to understand the operational modules established against various malicious events.

The test bed of multi-layered firewall architecture has been implemented for analyzing the Internet Protocol (IP) features. At this point, several firewalls are deployed among routers between source and destination. As shown in Figure 1, firewalls introduced in this section contain multiple sets of firewall rules that are distributed around the systems located in the network. The rule sets of various multi-layered firewall engines are defined under the primary case, secondary case, vulnerability case, and high precision case layers. In the first two case layers, firewalls identify the packet-based primary issues. In the next two layers, firewalls execute more vulnerable tests and more précised attack identification tests with the help of respective rule sets. Under this situation, this system is called a multi-layered (multi-level) firewall environment where it is distributed around the network.

Let us consider, "$s1$" and "$d1$" are sender and receiver respectively. Usually, firewalls are configured with "r" set of rules that are distributed to detect the attacks. In addition, the multi-level load-balancing firewalls equipped in this architecture distribute the packets and rule-based validation points "v." The handlings of distributed firewall policies allow three status options for each successful packet validation such as "block," "allow," and "skip rule set." The "skip rule set" option is newly introduced in this firewall policy for ignoring redundant rule executions for the same packet in the firewall architectures. In addition, the firewall model distributes the packet sequence load into multiple firewall units as same as active rule distribution to optimize the rate of energy consumption. The simplified architecture of multi-level firewall units "$f1 \ldots f4$" with distributed rule sets "$r1 \ldots r4$" are illustrated in Figure 1.

In the same manner, Rahman et al.[6] developed software-assisted cyber-physical security features in future-generation (6th-generation) wireless environments. Generally, the 6th-generation platform extends its path into massive industrial network applications, unmanned vehicle systems, wireless energy transfer, and other impactful future adaptations

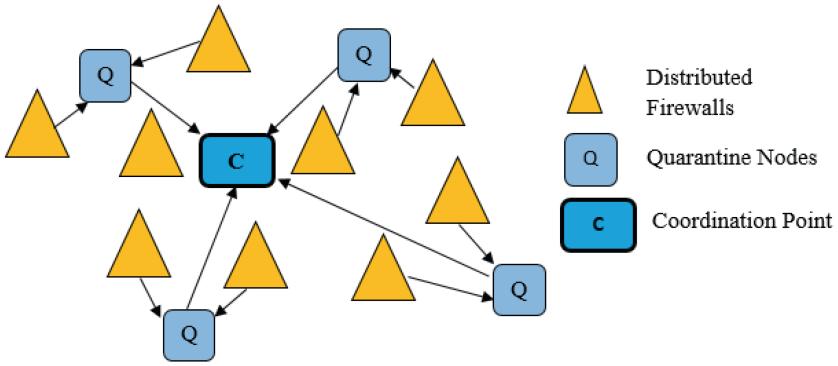

FIGURE 2 Spatial firewall deployment and quarantine points.

(410 MHz–6 GHz). In this environment, cyber security principles are playing a crucial role against intelligent attackers. In this regard, this work found security solutions based on security virtualization, artificial intelligence, and multi-point balanced monitoring phases. The idea behind the balanced and enriched security solutions in next-generation systems was analyzed to ensure energy considerations in the network. ElSawy et al.[15] created a spatially distributed firewall platform for wireless networks. Figure 2 shows the architecture of distributed spatial security systems.

The architecture shown in Figure 2 indicates the placement of multiple distributed firewalls (triangle nodes) and quarantine nodes (Q nodes). The deployment of Q nodes and a set of firewall nodes formed a secure cluster against malicious attacks in the network. On this basis, each firewall was initiated to monitor live network events to classify the attacks. As the firewalls were spatially distributed around the network, the computation load produced in each firewall system was massively reduced and the energy of each firewall node was optimally utilized. Notably, Q nodes placed under each cluster took the responsibility of sealing the malicious events as per the alerts raised from each firewall node. Hence the spatial firewall system ensured the benefit of load-distributed security principles. The experiment bed helped to understand the firewall observations in each cluster of the network.

Load distribution schemes and parallel architectures in cyber systems (firewalls) intensely optimize the computation complexity of monitoring points. From the discussion, this article identifies the crucial security benefits of multi-level firewalls[3] and spatial firewalls[15] than DL-assisted software-defined security policies in terms of computation load, accuracy, and error rate. Since the development of References 3,15 is idealized for distributed load-balancing solutions and lightweight attack detection policies, the DL-based standard security framework lacks performance. As same as load-balanced-security principles, energy optimization algorithms are expected through customized communication protocols, security protocols, packet classification strategies, and intrusion detection techniques. On the scope, a secure mobile edge platform was developed by Arif et al. to minimize the computation load in the network.

The computational offloading process in the mobile edge environment was considered a critical issue by this network model. In this case, this work proposed a Long Short Term Memory (LSTM) based load prediction model to eliminate the unfortunate network events. The security principles of the mobile environment were modeled through properly handled data streams and identified to improve the availability of network channels. The offloading prediction model analyzed the incoming data and dropped malicious (suspicious) events. In addition, this work extended its contribution to route the packets securely through Reinforcement Learning (RL) principles. This work computed transmission delay (uplink and downlink), computation latency, data size, and channel bandwidth to analyze the packet features using the LSTM engine. The successful analysis of present data stream characteristics constructed the prediction samples. As a result of the predicted data stream and suspicious offloaded data contents, the routing protocol had been assisted to form a path. Figure 3 illustrates LSTM-based protected routing practices. Security policies and firewall resources are deployed either at the software platform or hardware platform.

Considering the later solution, Srinivasavarma et al.[9] proposed ternary content addressable units (memory) and rule-point compression mechanisms for establishing hardware-based packet classification. In this work, packet headers were analyzed and classified according to compressed rule metrics. This work suggested the effectively compressed and encoded rule engines reduced the overall energy consumption rate in firewall systems. At the same time, the implementation of memory units in a fusion manner controlled the multi-packet classification processes under various network processing units. Figure 4 shows the design of rule encoding and compression schemes for energy-efficient firewall models.

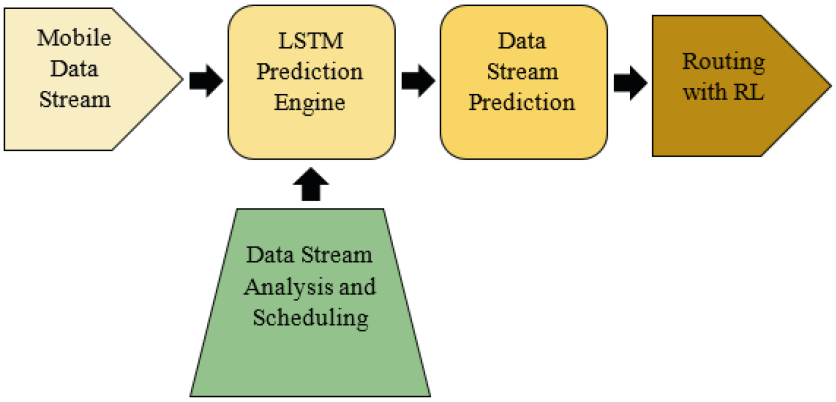

FIGURE 3 LSTM-based offloading and routing process.

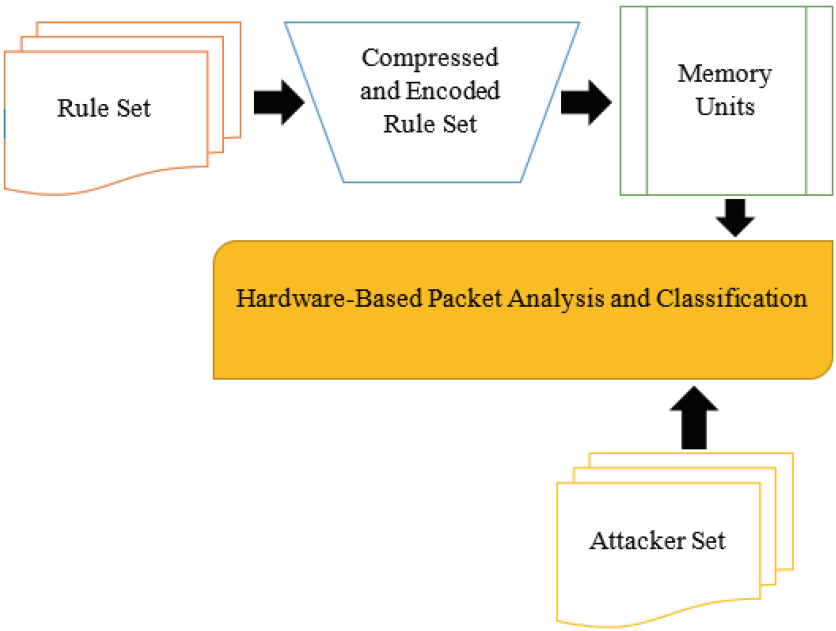

FIGURE 4 Hardware-based energy efficient firewall system.

Similarly, the packet classification rules are illustrated in Table 2. In general, these rules were encoded with numerical data to be mapped with the packet header details and characteristics. Yi et al.[12] proposed green firewall principles to isolate real-time intrusions through minimal computation overhead and energy optimization strategies. This work mainly monitored the node's energy consumption rate during data transmission and intrusion prevention periods. The implemented alarm system of the green firewall was operated to minimize energy wastage. In the same manner, Demirci et al.[28] applied virtualization-based security principles in software-defined networks for managing energy-efficient security conditions. Virtualizing the network security functions around the network environment is a notable idea to isolate the attack features and balance the computation load. Under this security model, the virtualization functions were configured to build secure fifth-generation transmission paths (Figure 5).

Energy-efficient wireless communication systems are widely expected around the world to manage future-generation networks. In this manner, Kumar et al.[33] provided a detailed analysis of energy-efficient policies in underwater sensor networks. As underwater communication channels are considered with characteristics such as acoustic channel models, autonomous node management, failure management, energy-efficient models, and bandwidth management.

Unlike terrestrial wireless sensor networks, underwater sensor networks are heavily affected due to water channel distortions and frequent signal attenuation possibilities. According to the energy-saving expectations, various network characteristics were considered as given in Figure 7. As shown in Figure 6, distributed routing protocols' contribution and quality metrics are significant for energy-optimized underwater channel management principles.

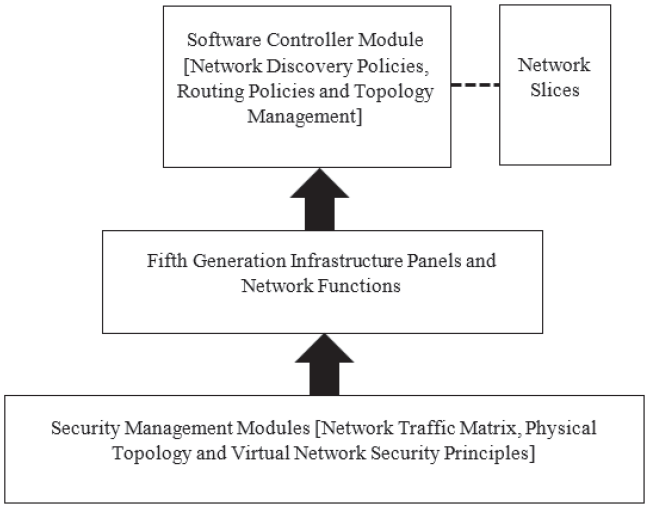

FIGURE 5 Energy-optimized-network virtualization and security management policies.

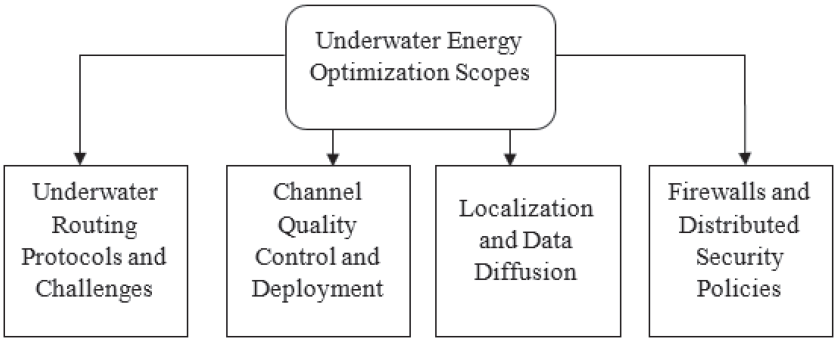

FIGURE 6 Underwater energy related characteristics and security policies.

In the same manner, the successful identification of node locations and routing paths through vulnerable channels ensures the betterment of the network protection rate.

Particularly, the distributed firewall policies in the underwater sensor networks are expected with good channel management system, routing policies, and other quality metrics. These significant characteristics were effectively discussed in the work. This article identifies that improper energy utilization and energy wastage lead to a lack of security benefits in wireless networks. Particularly, next-generation firewall rule engines and security frameworks are highly expecting green electronic environments to monitor suspicious attacks in the network. In common, wireless networks are more vulnerable to various types of malfunctions than strongly developed wired networks. In this case, the effective understandings of energy controlling mechanisms and energy distribution mechanisms help to improve the quality of wireless network security platforms.[36-38] Based on these observations, the energy-optimized-security (firewall) mechanisms are categorized as energy-saving strategies and computation load-balancing strategies.

The performance metrics such as energy consumption rate, secure packet delivery rate, suspicious event detection latency, system accuracy rate, false positive rate, and computation overhead are considered for evaluating the existing techniques. As discussed, the existing techniques are comparatively analyzed under the load-balancing act and energy-saving act independently. Anyhow, both acts focus on energy optimization rules around the distributed wireless environment in each node. The performance metrics are defined as follows.

$$\text{Energy consumption rate} = \text{Energy spent at time } `t1' \text{ (Joules)}, \tag{1}$$

$$\text{Secure packet delivery rate} = \frac{\text{Packet delivery rate (normal)}}{\text{Packet delivery rate (malicious)}} \times 100, \tag{2}$$

$$\text{Secure accuracy rate} = \frac{\text{Number of attacks identified correctly}}{\text{Total number of packets received}} \times 100, \tag{3}$$

$$\text{False positive rate} = \frac{\text{Number of false attack detections}}{\text{Number of false attack detections} + \text{Number of actual negative detections}} \times 100, \tag{4}$$

$$\text{Computation overhead} = \frac{\text{Additional tasks operated at time '}t1\text{'}}{\text{Average number of tasks executed}} \times 100, \tag{5}$$

$$\text{Event detection latency} = \text{Time taken to detect intrusion (milliseconds)}. \tag{6}$$

As given in Equations (1)–(6) the performance metrics are calculated for proving the ability of existing security mechanisms under the prescribed testbed environment (Table 4). Tables 5 and 6 illustrate the average energy consumption rate of energy optimization strategies and load distribution strategies respectively. Particularly, the comparison of average energy drops among wireless nodes due to the internal security functions.[39-41] The energy consumption rate of each wireless node is calculated on behalf of network monitoring services, packet classification procedures against possible attacks vary as the number of nodes increases in the network. In this experiment, this article assumes that the number of peer nodes is directly proportional to the number of packets transmitted in the network. On this basis, the number of nodes is increased from 100 to 500 to observe the performance of notable works. In this comparison, the energy-efficient security mechanisms attain moderate energy consumption rates from 18.99 to 20.12 (J) according to their design strategies under the wireless network of 100 nodes.[9,33,35] Particularly, the underwater security mechanisms[33] and MUSK framework for wireless sensor networks consume minimal energy wastage. As the mechanisms are developed for resource-limited wireless nodes, the crucial expectation of energy optimization has been achieved better compared to other systems.

As the number of nodes gradually rises from 100 to 500, the maximum energy consumption rate is recorded for a high computing framework (SDN)[28] based on both secure network management and routing functions. At the same time, other works are slightly affected due to the highly populated network environment.[12,19] As given in Table 5, the experimental functions of C3 provide the distributed computational task offload and migration solutions to reduce energy wastage in the mobile edge platform. In this regard, the average energy optimization rate of C3 is comparably better than C4,[9] C5,[12] C5,[19] and C8[28] as the successful adaptation of LSTM-based process discrimination layers. Comparing the techniques C3, C9,[33] and C10,[35] C3 used the fusion of RL and LSTM to ensure optimal routing and a multi-level lightweight computation

TABLE 5 Energy optimization strategies—average energy consumption rate.

Number of wireless nodes	C3	C4[9]	C5[12]	C7[19]	C8[28]	C9[33]	C10[35]
100	19.88	20.12	23.79	20.57	22.33	19.23	18.99
200	23.18	24.45	27.94	27.12	26.78	21.36	20.24
300	26.36	27.42	30.13	28.89	28.93	24.11	22.77
400	28.81	29.22	30.49	29.33	31.56	26.62	24.91
500	31.45	32.71	31.16	30.71	32.62	29.79	27.63

TABLE 6 Load-balancing strategies—average energy consumption rate.

Number of wireless nodes	C1[3]	C2[6]	C6[15]
100	18.28	20.11	16.34
200	20.92	22.38	17.04
300	23.57	25.15	17.46
400	23.85	27.74	19.16
500	25.09	30.41	21.82

analysis process. Due to these aspects, the neural functions of this system enable optimal energy security and network protection in wireless networks.

In this case, C10[35] proposed energy-efficient attack detection systems using MUSK (derived from authors' names) architecture. This architecture used cluster head-based intrusion report analysis for initiating alert messages. In this architecture, each wireless sensor node monitored the neighbor events to detect intrusions and cooperate with local cluster heads. The monitoring nodes or MUSK agent nodes send reports to cluster heads and cluster heads send the valid report to the base station. The distributed intrusion detection principles proposed in this work were implemented to ensure the wireless sensor nodes. As compared to C9[33] and C3, this work generates minimal energy consumption to manage the distributed sensor node's security. Similarly, C1,[3] C2[6] and C6[15] techniques are ranges of energy consumption rates based on load-balancing strategies. In the same manner, Table 6 gives the best load-sensitive security mechanisms as C1[3] in terms of load distribution and multi-firewall principles (number of nodes is 100). Particularly, this is a dynamic packet distribution mechanism with multi-packet evaluation rules (local firewall principles and internet firewall principles) for improving energy-saving solutions.

In this regard, this work produces 18.28 J as a minimal energy consumption rate where the network has been populated with 100 nodes. The load distribution scheme uses traffic transformation algorithms that manage multiple firewall rules. Anyhow the energy consumption rate of C6[15] is still minimal as it uses spatially distributed firewall engines to quarantine the suspicious events. Particularly, the spatial firewalls implemented in a testbed are using cyber-physical security approaches. In this mechanism, a large-scale distributed network has been configured with quarantine vaults and distributed firewall rules. As this work distributes the network events among various vault sections, the energy consumed by each node is limited continuously. Thus the C6[15] produces the range of energy consumption between 16.34 and 21.82 J as the number of nodes varies from 100 to 500.

A spatial firewall[15] system is an effective idea for improving the security standards for large-scale wireless networks.[42-44] In addition, the applications of spatially distributed firewall systems among the entire network ensure even security solutions and minimize unwanted energy overhead in each node. Hence, the average energy consumption of a spatial firewall system[15] assures a reasonable energy rate from 16.34 to 21.82 (J) as nodes are populated from 100 to 500. In comparison, the deep learning-based security models produce better protection yet the energy required to implement the procedures is more compared to C1[3] and C6.[15] Similarly, Tables 7 and 8 depict secure packet delivery rates achieved from existing security principles amid vulnerable network activities. In this concern, Table 7 denotes the energy

TABLE 7 Energy optimization strategies—secure packet delivery rate.

Number of live channels	C3	C4[9]	C5[12]	C7[19]	C8[28]	C9[33]	C10[35]
30	25.56	25.23	26.11	24.78	27.78	26.12	23.78
60	25.66	25.18	27.12	24.56	28.26	26.11	23.87
90	26.98	25.63	28.13	26.92	27.99	25.45	23.61
120	29.12	25.91	30.12	28.51	29.23	25.19	23.98
150	29.44	26.98	29.19	28.83	30.18	27.11	24.11
180	29.15	27.67	29.18	28.99	28.44	27.91	22.74

TABLE 8 Load-balancing strategies—secure packet delivery rate.

Number of live channels	C1[3]	C2[6]	C6[15]
30	28.12	27.43	27.99
60	27.98	28.11	28.92
90	29.12	30.27	30.22
120	30.45	30.58	29.15
150	30.23	29.34	30.24
180	30.91	30.15	29.86

optimization-based security policies' performance, and Table 8 denotes the load-balancing based security policies' performance. As discussed, the security policies contain both effective firewall principles and internal (In-Node) evaluation traffic analysis procedures. According to that, the secure packet delivery ratio states the ratio between the number of packets successfully delivered to the destination and the total number of packets populated in the network amid a malicious environment. Table 7 shows the average performance of hardware-based packet classification rules,[9] underwater firewall principles,[33] and MUSK-based secure sensor network development strategies[35] than other security mechanisms.

Under the observation, these security mechanisms get packet delivery rates between 22.74 and 27.67 kbps as they are contributing to a restricted and resource-limited network environment. On the other side, LSTM-based security principles, green firewall principles,[12] and context-sensitive security principles[19] attain notable progress in delivering the packets securely among the limited set of nodes. The rate of these techniques in secure packet delivery ranges from 26 to 30 kbps approximately. In this comparison, the based energy optimization technique is gradually attaining its maximum secure packet delivery ratio as the number of training sessions increases over time. As the number of live channels is increasing in the network, the need for LSTM-RL fusion helps to ensure a better packet delivery rate among attackers.

In the same manner, the green firewall mechanism is suitable for wireless sensor network environments for attaining optimal secure throughput rates. At the same time, this mechanism does not suit other large-scale wireless networks. On the other side, context-aware security mechanisms and software-defined network principles produce a moderate packet delivery rate. In this case, the data context analysis with load analysis procedures is helpful to improve energy-saving plans yet limited under safety measures compared to earlier techniques. The software-defined security rules with traffic mechanisms are mainly made for mobile network environments. Anyhow, this mechanism ensures a reasonable secure packet delivery rate under the proposed simulation environment.

This shows the stability of the network system against malicious issues and energy wastage. Table 8 mentions the observations of load-balanced security mechanisms in terms of secure packet delivery rate between.[3,6,15] In this analysis, the multi-level packet analysis model[3] spatial firewall principles[15] and deep learning-based wireless security model get a maximum secure packet delivery rate of nearly 31 kbps with minimal variations as the number of live channels varies from 30 to 180. The technical aspects of multi-level firewall systems are more sophisticated and complex packet analysis procedures are increasing the intrusion identification rate. Consequently, the secure packet delivery rate is identified as 30.91 kbps against a maximum number of live channels in the network. At the same time, spatial firewall systems and deep learning-based security principles are competing with each other to get the maximum secure packet delivery rate. In this case, a deep learning-based framework gets a better rate as compared to a spatial firewall model. Though spatial firewall security principles attain a minimal energy consumption rate, they fall slightly in terms of security metrics against the deep learning approach. As the learning system of deep neural networks optimizes the detection of possible attacks in the network rather than spatial firewall models, it achieves a good secure throughput rate.[26,45-47] In extension, Tables 9 and 10 describe the comparative analysis between existing security models using event detection latency (milliseconds [ms]) against increasing number of packets.

As the number of packets increases from 185 to 290, a gradual hike in event detection latency is detected for different mechanisms. The event detection latency can be defined as the average time taken to detect suspicious attacks in a communication session by extracting the features of packets.[48-50] The latency is calculated as given in Tables 9 and 10 under 500 node circumstances. In this experiment, the minimal and maximum latency has been achieved as 221.98 ms[9] and 256.98 respectively when analyzing 185 data packets total in an iteration. Similarly, the minimum and maximum bounds

TABLE 9 Energy optimization strategies—event detection latency.

Number of packets received (500)	C3	C4[9]	C5[12]	C7[19]	C8[28]	C9[33]	C10[35]
185	256.98	221.98	241.34	242.12	255.98	239.35	240.11
267	267.14	224.56	248.92	248.99	266.62	244.95	246.67
378	298.33	238.12	252.13	259.36	284.57	249.23	250.55
166	309.28	242.16	266.47	270.49	295.54	255.51	257.34
355	320.14	259.69	272.58	281.82	309.12	261.37	262.28
400	331.11	260.18	280.83	287.77	311.19	268.84	269.93
290	350.21	277.89	291.15	301.65	329.46	273.36	274.22

TABLE 10 Load-balancing strategies—event detection latency.

Number of packets received (500)	C1[3]	C2[6]	C6[15]
185	235.12	256.78	249.98
267	239.19	269.49	262.56
378	246.78	278.33	274.41
166	258.81	285.61	281.09
355	266.17	300.04	292.36
400	273.48	309.17	301.87
290	299.84	320.16	313.69

of latency have been recorded under the load of 290 packets are 277.89[9] and 350.21 respectively. As compared to the event detection latency (milliseconds) of various techniques (Tables 9 and 10), the minimal latency has been identified for lightweight security techniques rather than machine learning-based techniques and large-scale networks.

In addition, security principles made for sensor network environments and underwater network achieves minimal latency than other complex networks. In another way, Table 9 indicates the minimal latency for C4[9]-hardware-based multi-packet classification mechanism. Compared to other techniques, the hardware-located engines support better security solutions than software-based mechanisms. In the same manner, the comparison between Tables 9 and 10 shows the minimal latency to detect intrusions for C1[3] which is next to C4.[9] As C1[3] executes distributed load management strategies for multi-firewall policies, the time taken to detect intrusions around the network is shared and reduced. Thus this system achieves its minimal range of event detection latency between 235.12 and 299.84 ms. At the same time, the minimal latency observed in this work may not lead in to maximum accuracy of attack detection for all mechanisms.

In Figure 7, it is noted that the hardware-based multi-classification principles,[9] context-aware security frameworks,[19] and energy-efficient intrusion detection models[35] produce better system accuracy rates from 97% to 98% for analyzing 185 packets in a session. The accuracy rate of security systems against any attack is defined as the ratio between correctly detected attacks and the total number of packets received. Similarly, the rate declined between 92% and 93% for 290 packets. At the same time, Reference initiates LSTM-based computational load management techniques for initiating security procedures. Compared to earlier works, LSTM finds and analyzes the sequence of security parameters and communication data to detect suspicious events. However, the accuracy is slightly reduced as LSTM functions handle complex security models and load analysis procedures. In contrast, Reference 12 provides suitable energy-efficient firewall procedures for WSNs. The procedures initiated in each sensor node are mainly implemented for a lightweight computing environment. At the same time, it lacks accuracy (89%) in attack detection due to standard intrusion detection policies even though the procedures maintain an optimal energy distribution rate.

In the comparison, Reference 28 implements software-defined security policies for fifth-generation networks and energy-optimized routing schemes. In the experiment, it is detected that the execution of security procedures is mainly related to high-speed mobile communication networks rather than lightweight policies. The involvement of fifth-generation (5G)-based security rules directs the network functions to secure the internet environment (heterogeneous models). Though the development of security policies is useful against various attacks in 5G networks, these functions have restricted computational benefits in resource-limited nodes. Due to these reasons, Reference 28 falls in detection accuracy. On the other side, Reference 33 performs notably as the system can secure the underwater wireless nodes. The characteristics of underwater nodes are limited memory, acoustic signaling model, high interference rate, and limited power efficiency. In this experiment, the firewall procedures developed for the nodes maintain more fault-tolerant policies. The development of lightweight firewall policies run in each node takes distributed decisions based on internal rules.

Each node in the underwater environment is capable of handling a sequence of packets and executing firewall rules. This environment gradually divides the load and finds the attacks. Due to this reason, this scheme gives comparably better detection accuracy (93%) than.[12,28] The betterment of energy-efficient security principles such as References 9,19,35 is achieved through crucial development strategies under multi-validation procedures. In this experiment, the first technique[9] has been implemented in a hardware environment with multi-level packet classification rules. In the same manner, second[19] and third[35] techniques are implemented for imposing distributed security architectures. These techniques get better accuracy in intrusion detection as they are efficient and complex in nature.

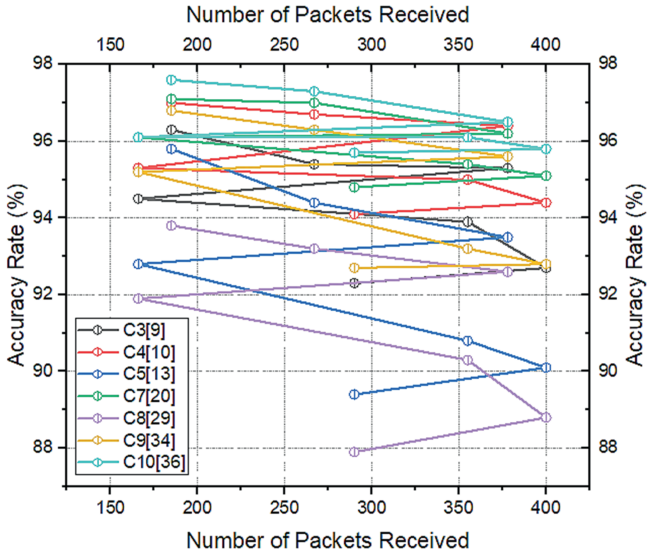

FIGURE 7 System accuracy rate—energy optimization strategies.

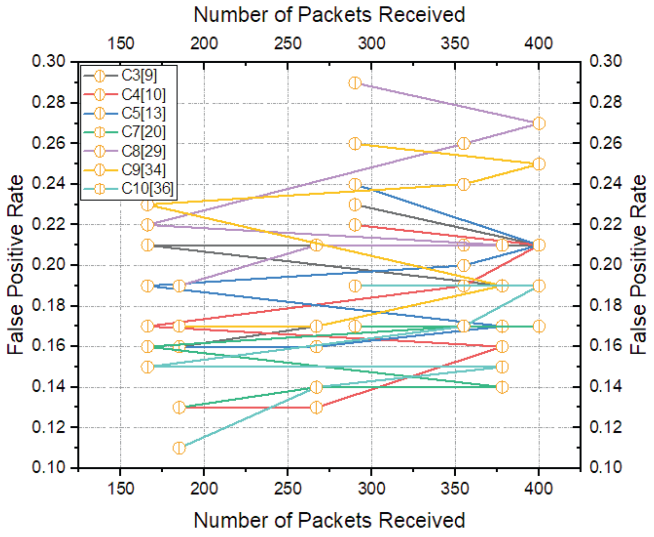

FIGURE 8 False positive rate—energy optimization strategies.

The experimental study is deeply extended for validating other performance metrics such as system accuracy rate and false positive rate. In this connection, Figure 8 gives the comparative results of energy optimization-based security techniques in terms of false positive rate over the number of packets received. The detection of falsely raised positive alarms for legitimate events is calculated for References 12,28,33. In this comparison, the observations of accuracy resemble each work. In the same manner, the false positive rate is calculated for the occasions of wrongly raised attack indications on legitimate packets in the network.[51-53] The improvement of any decision-making system finds a minimal false positive rate to ensure minimal tolerance. According to that, Figure 8 gives minimum false positive rates for References 9,19,35 as these mechanisms find multi-class packet analysis frameworks under energy-controlled environments compared to other techniques. Similarly, the observation of other techniques gives the false positive rate from 0.25 to 0.29 as crucial downtime in the network. Though other techniques spend minimal energy and latency in the vulnerable network, the optimal security performance is achieved through complex or multi-level packet analysis rules only. Thus the existing techniques such as References 9,19,35 attain good performance in the testbed environment.

In the same way, the metrics such as system accuracy rate and system error rate are used for analyzing the performance of load optimization strategies for enabling extended security activation span. The details are illustrated in

Figures 9 and 10. As given in Figure 9, the system accuracy rates of References 3,15 are better than deep learning-assisted software-defined procedures. The reason for observing a better accuracy rate (99%–93.5%) for the above works is stated with the help of optimal load distribution and spatial load distribution mechanisms. In the same manner, the deep learning-based security principle performs optimally yet it is not flexible under distributed scenarios.[6] According to the observations, Figure 10 illustrates the minimal and maximum error rate from 0.11 to 13.1 in connection with References 3,6,15 respectively. The error rate shall be denoted as 1-accuracy rate.

In this comparison, the multi-firewall network establishment[3] through load distribution policies attains a maximum system accuracy rate than other techniques. The strategy of this security scheme focuses on optimal solutions using lightweight firewall agents. Though this work has not been developed using any machine learning techniques, the effective placement of load-balanced firewall models achieves good accuracy in attack detection. Next to this technique, the spatial firewall[15] are following the same type of distributed attack detection policies to increase the accuracy rate. The experimental observations discussed above show the system performance through various metrics against changing network parameters under various iterations.[54-56]

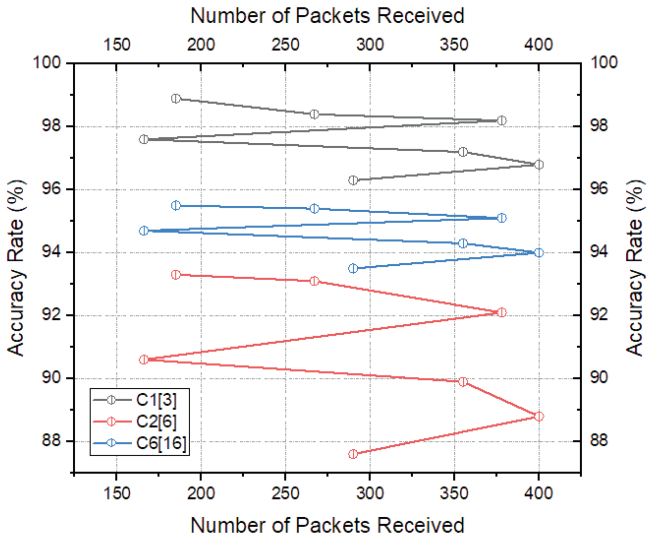

FIGURE 9 System accuracy rate—load optimization strategies.

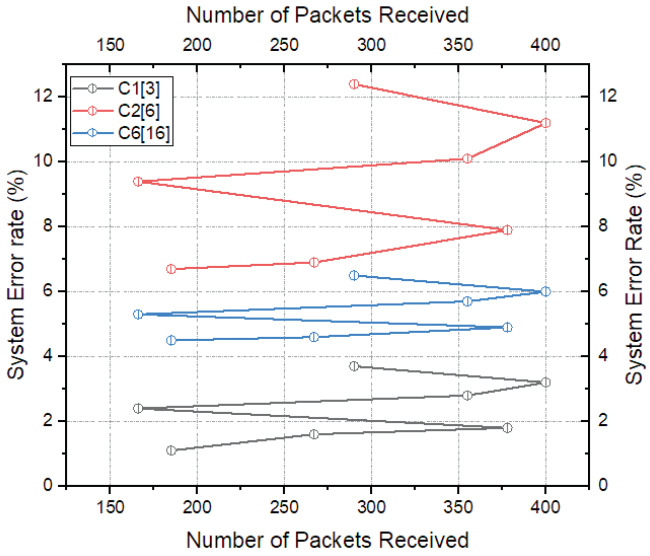

FIGURE 10 System error rate—load optimization strategies.

Anyhow, the identification of computation overhead confirms the system performance in a testbed platform. The computation overhead shall be expressed as the amount of excessive tasks required over the usual tasks handled by the system. Tables 11 and 12 present the computation overhead rate (%) of energy-optimized security principles and load-balanced security principles respectively.

This experiment has been iterated from 10 to 60 times to get the average performance of each security model to counter the attacks. The comparison taken between various approaches shows that the load-balanced security mechanisms (firewall strategies) ensure optimal overhead than simple energy-optimized security mechanisms.[57-60] In this observation, computation overhead is shared or reduced in the multi-level distributed security mechanisms such as References 3,9 compared to other techniques.[61-63] At the same, other load-balancing techniques reduce the computation overhead as they are specially implemented for controlling the workload. On the other side, energy-optimized security principles and firewall management systems mainly target energy-saving principles rather than load-reduction policies. Thus, the existing techniques shown in Table 11 are producing higher computation overhead than load-balancing techniques. Accordingly, the overall experimental study shows the benefits and limitations of notable research works.[64-66]

In the concern, Table 13 illustrates the recent works carried out on resource-efficient security policies for ensuring energy safety in the networks. Manman et al.[67] proposed dynamic clustering methodologies for optimizing computation load and energy load around the IoT-based networks. In this mechanism, ANN procedures are implemented with backpropagation policies to analyze the energy parameters of IoT nodes. Based on energy classification results, clusters have been created and organized in a distributed manner. Generally, IoT devices are heterogeneous in terms of size, power sources, energy limits, transmission range, processing capability, interfaces, application tools, and sensors. In this case, back-propagated ANN functions help to classify nodes based on learned parameters and deliver decisions for optimal clustering steps. Unlike conventional Low-Energy Adaptive Clustering Hierarchy (LEACH), back-propagated ANN reduces the error rate in node selection for individual clusters. The experimental base of this work has a different set of IoT nodes with uneven configurations. Each node in the network initiates internal ANN-based clustering functions for grouping dynamic and energy-efficient nodes as clusters. The observations show that the ANN functions effectively reduce node-level computation load and energy wastages.

He et al.[68] initiated a detailed survey on energy-efficient security functions for resource-limited nodes. Particularly, the survey identifies the notable ways of managing security initiatives in mobile nodes and wireless sensor nodes. These types of nodes are generally deployed at hostile regions and environmental points. In this situation, the nodes are prone

TABLE 11 Energy optimization strategies—computation overhead.

Number of iterations	C3	C4[9]	C5[12]	C7[19]	C8[28]	C9[33]	C10[35]
10	9.9	5.6	8.3	8.8	8.9	7.3	7.9
20	11.2	6.3	8.5	9.4	9.5	7.7	7.9
30	11.5	5.9	8.6	9.5	9.9	7.5	8.2
40	10.9	5.5	8.1	8.9	9.7	7.1	8.6
50	11.2	5.9	8.6	9.2	10.4	6.8	8.4
60	10.8	6.3	8.4	9.5	10.3	6.9	7.7

TABLE 12 Load-balancing strategies—computation overhead.

Number of iterations	C1[3]	C2[6]	C6[15]
10	5.4	6.4	5.9
20	5.6	6.3	6.2
30	5.7	6.7	6.6
40	5.6	6.9	6.9
50	5.9	6.9	6.7
60	6.1	7.2	6.4

TABLE 13 Literatures—resource sensitive security policies.

No.	Articles	Methodologies	Research problems and solutions	Limitations
1	Manman et al.[67]	Dynamic clustering mechanisms for IoT environment using Artificial Neural Network (ANN).	Identifying and creating dynamic clusters by considering energy limits and information correlation using a back propagation neural network.	Dynamic clusters are efficient yet the adaptation of security principles may be considered to manage clusters.
2	He et al.[68]	An extended survey on energy-efficient security procedures that are suitable for resource-limited networks (mobile networks and WSNs).	Analyzing the energy optimization procedures at different levels such as node internals, interfaces, network architecture, and security measures against multiple attacks.	Theoretical analysis and multi-level discussions are conducted. However, experimental justifications shall be provided.
3	Liu[69]	Router-based firewall principles with effective design considerations.	Avoiding the limitations of terminal node-based firewall procedures and imposing network router-based firewall mechanisms.	Testbed/Experimental discussions and justifications shall be provided rather than comprehensive details.
4	Durga Bhavani and Mangla[70]	Comparative analysis of various intrusion detection mechanisms that are optimal for resource-limited IoT systems.	Classifying and understanding the models of different types of intrusion detection procedures against suitable attack issues.	Comprehensive discussions are conducted yet the practical benefits shall be included.
5	Abba Ari et al.[71]	A deep analysis of security and privacy considerations among multiple vulnerable points/breaches in cloud IoT.	Suggesting proper security solutions for enabling protected sockets, shells, web channels, and ports. In addition, providing more energy-optimized security mechanisms is the major contribution.	This is an informative security-based analysis. However, this work shall be extended into edge and small-scale networks.
6	Brahmam and Anand[72]	Cloud-based virtual machine load distribution and energy saving principles.	Managing the migration of virtual machines of cloud network with optimal load distribution model. Through the model, the cloud network optimizes the energy level in each virtual machine. In this experiment, the span-based scheduling algorithm and deep learning network algorithm.	Computations used for cloud-based deep learning principles increases the internal load of the network.
7	Mahmood et al.[73]	Practical evaluation of omni-secure firewall policies in private cloud networks.	Providing the efficiency and limits of resource-limited private cloud firewall policies against DDoS attacks, and distributed attacks.	Machine learning and deep learning-based data processing techniques are applied yet these procedures may cause excessive response time.
8	Kurek and Macko[74]	Host identity Protocol Tunnel is created to enable secure channel/communication between resource-limited IoT devices and servers.	Defining the characteristics of data packet security parameters and initiating control message exchanges to validate host identities. Supports both internet protocol versions 4 and 6.	Communication load and timing issues shall be discussed.

to energy wastage and other capabilities. On the scope, the survey analyzes the limits of network architecture, node parameters, channel qualities, interfaces, maximum energy limits, and possible security provisions. In the end, this survey suggests lightweight security mechanisms such as secure hashing, block chippers, message authentication codes, and rule-based policies for protecting the nodes.

Liu et al.[69] proposed router-based network firewall policies with energy-efficient design considerations. Compared to terminal-based firewall tools, internal firewall devices ensure more security in the interconnected network environment. According to the expectation, routers in the network are configured with internal firewall security policies to monitor internet datagrams. The experimental setup of this work has multiple routers among the terminal nodes. Routers are enabled to connect multiple local networks (communication nodes and terminal nodes) and are configured with packet-filtering firewall rules. On the platform, the entire network has been secured internally and externally compared to conventional mechanisms. At the same time, the computation load is slightly increased in the router points as they are executing both routing and packet filtering tasks at the same time.

Durga Bhavani and Mangla[70] and Abba Ari et al.[71] take a comparative survey on IoT-based security principles using intrusion detection and privacy policies respectively. In both surveys, a resource-limited IoT environment is considered for experimenting energy energy-efficient security mechanisms. In Reference 70, intrusion detection techniques such as signature-based, anomaly-based, and statistical-based are discussed to find suitable IoT-related solutions. In this discussion, the survey justifies that distributed agent-based intrusion detection techniques are more suitable for energy-efficient security principles. At the same time, Reference 71 exposes the vulnerability analysis and privacy establishment opportunities for IoT systems. According to this survey, vulnerable points of the network are insecure ports, shells, interfaces, and suspicious user activities. Based on this survey, energy-efficient security and privacy preservation policies enabled in each IoT element are possible through tiny node-based agents rather than complex processes.

Brahmam and Anand[72] proposed cloud-based virtual machine security mechanisms and load management policies. On the motivation of virtual machine security principles, cloud-based computation load estimations, and deep learning-based parameter classification procedures are implemented. The implemented procedures in each virtual machine of the cloud network initiate data collection, characteristics analysis, and virtual machine load estimation tasks. At the testbed, each virtual machine parameters are used to train the deep neural network engines to decide the load distribution rate in the cloud. In addition, this work drives the motive to identify a more efficient way of energy optimization in each virtual machine. Generally, virtual machines are deployed with limited resources compared to the physical machine in the cloud, this deep neural network-based proposed model ensures better performance in terms of computation time, overhead, energy wastages, and space complexity.

Similarly, Mahmood et al.[73] proposed machine learning-based common firewall systems for private cloud environments. According to this proposed technique, private cloud networks are targeted by resource-exhausting attacks such as DDoS, and malfunction attacks. Against these attacks, the machine learning algorithms make an efficient learning-based decision by minimizing practical errors. On the scope, DDoS and other distributed attacks raised to halt cloud functions are classified in a distributed manner in each host. By the way, the experiment of the model ensures the stability of the cloud network against attacks via metrics such as packet drops, true positives, and throughput improvement rate. In the domain, Kurek and Macko[74] developed an optimized host identity protocol-based secure tunnel for exchanging data packets between IoT devices. As IoT devices are more unstable against resource wastages, the involvement of host identification-based security benefits makes more convenient data communication. At the same time, the implementation phase of the host information protocol in each device admits the valid identities only through internet channels. Tables 14

TABLE 14 Memory overhead-resource-limited security policies.

Number of iterations	R1[69]	R2[72]	R3[74]
10	6.7	5.2	4.5
20	7.7	7.1	6.1
30	8.9	6.8	5.7
40	7.8	6.6	5.8
50	8.3	6.9	6.2
60	8.1	7.4	6.4

TABLE 15 Time complexity-resource-limited security policies.

Number of iterations	R1[69]	R2[72]	R3[74]
10	0.32	0.29	0.25
20	0.39	0.36	0.33
30	0.41	0.34	0.31
40	0.40	0.36	0.31
50	0.45	0.37	0.32
60	0.46	0.41	0.33

and 15 show the memory overhead and time complexity rate of recently inducted security practices for resource-limited networks (Table 2). In this experimental setup, each node in the network (virtual machine, IoT device, and routing node) takes its security procedures. As a result, the router-based firewall policies, R1[69] are consuming more overhead in time and memory plane. The reason for obtaining more load in the routing point is integrating both routing protocol and firewall functions. At the same time, R2[72] produces moderate overload at each security point. In this work, virtual machines are engaged with firewall security rules in the cloud network. In addition, the cloud-based energy-efficient model has been governed by classified decisions of deep neural networks.

In this experimental comparison, R3[74] provides more suitable energy-efficient security solutions for IoT-based devices. In this experiment, IoT devices are created with a different set of internal parameters. The energy-efficient open host identity protocol runs in each IoT device and optimizes the process of valid packet transmissions. In contrast, the protocol blocks other suspicious packets coming from malicious nodes. Compared to other security policies, R3[74] works with more lightweight distributed functions since the devices are tiny in the network. From the discussions, this article ensures the importance of security buildups among resource-limited networks such as mobile nodes, sensor nodes, private cloud nodes, virtual machines, and IoT devices. The experiments conducted on these discussed techniques help to observe the possibilities of various network-specific firewall/security policies and node-specific security policies.

From the experimental findings, this article suggests both load-balanced security mechanisms and energy optimization algorithms can be chosen for increasing the network lifetime and availability time. Particularly, this article suggests implementing low-powered energy optimization algorithms to manage sensor-based security needs. At the same time, it is advisable to improve the quality of security mechanisms using machine learning techniques (LSTM-RL) and deep learning techniques for resourceful wireless networks. In addition, the results observed from various experiments reveal the important benefits of distributed network intrusion detection principles and firewall (multi-level) configuration principles to get optimal security benefits. From the conducted survey, this article suggested the way of energy-optimized security mechanisms and firewall policies for networks with limited resources. Specifically, the techniques discussed in the article state the flexibility in load-balancing solutions, resource-sensitive security operations, and lightweight distributed firewall principles for protecting wireless networks. Based on the assumptions, the survey finds security opportunities to build energy-efficient outdoor wireless networks and distributed firewall deployment methods.

4 | CONCLUSIONS

The understanding and experimental studies on security principles give a future idea for improving the stability of networks against suspicious events. Particularly, energy optimization and load distribution schemes applied for classifying the packets impact the lifespan of network functions. In this connection, the security frameworks are established as intrusion detection systems, firewall engines, and other security models for wireless networks. Notably, firewall points or any security models are deployed either at a central location or distributed locations. Considering all conditions and deployment strategies, this article provided a detailed experimental study between load-balanced security provisions and energy-controlled security provisions for protecting wireless networks. From the experiments, it was observed that the load-balanced security features (distributed) were suitable for resource-limited wireless networks with minimal computation load. In contrast, the centralized or multi-class firewall rules were operated effectively to assuring optimal security solutions.

Based on the experimental discussions, we found the need for green computing principles, energy-optimized security features, security benefits for tiny nodes, and energy-optimized firewall rules in wireless networks. In this connection, the future direction is expected with more crucial and application-specific energy management techniques that are producing long-lasting benefits of secure data communication through wireless channels. In addition, these future practices assure the stability of wireless channels against attacks.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

ORCID

S. A. Sivakumar https://orcid.org/0000-0001-8558-9843
M. Jahir Pasha https://orcid.org/0000-0002-8309-8845
Jaime Lloret https://orcid.org/0000-0002-0862-0533

REFERENCES

1. Togay C, Kasif A, Catal C, Tekinerdogan B. A firewall policy anomaly detection framework for reliable network security. *IEEE Trans Reliab*. 2021;71(1):339-347.
2. Anwar RW, Abdullah T, Pastore F. Firewall best practices for securing smart healthcare environment: a review. *Appl Sci*. 2021;11(19):9183.
3. Durante L, Seno L, Valenzano A. A formal model and technique to redistribute the packet filtering load in multiple firewall networks. *IEEE Trans Inf Forensics Secur*. 2021;16:2637-2651.
4. Liu AX, Li R. Collaborative enforcement of firewall policies in virtual private networks. *Algorithms for Data and Computation Privacy*. Springer, Cham; 2021:139-170.
5. Al-Haija QA, Ishtaiwi A. Multiclass classification of firewall log files using shallow neural network for network security applications. *Soft Computing for Security Applications*. Springer, Singapore; 2022:27-41.
6. Rahman MA, Hossain MS. A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective. *IEEE Wirel Commun*. 2022;29(2):52-59.
7. Setiawan Y, Sembiring A, Arif M, Wihdayati W. Analysis and design wireless network and security based on firewall in pit mining area PT ABC. *Syntax Liter Jurnal Ilmiah Indonesia*. 2022;7(4):3935-3946.
8. Diansyah TM, Faisal I, Perdana A, Sembiring BO, Sinaga TH. Analysis of using firewall and single honeypot in training attack on wireless network. *J Phys Conf Ser*. 2017;930(1):012038.
9. Srinivasavarma VS, Pydi SR, Mahammad SN. Hardware-based multi-match packet classification in NIDS: an overview and novel extensions for improving the energy efficiency of TCAM-based classifiers. *J Supercomput*. 2022;14:1-36.
10. Zhang Y. Research and application of next-generation firewall technique in medical network. *J Comput Methods Sci Eng*. 2022;22:1461-1476.
11. Akin O, Gulmez UC, Sazak O, Yagmur OU, Angin P. GreenSlice: an energy-efficient secure network slicing framework. *J Internet Serv Inf Secur*. 2022;12(1):57-71.
12. Yi P, Zhu T, Zhang Q, Wu Y, Li J. Green firewall: an energy-efficient intrusion prevention mechanism in wireless sensor network. *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE; 2012:3037-3042.
13. Schwarz F. TrustedGateway: TEE-assisted routing and firewall enforcement using ARM TrustZone. *25th International Symposium on Research in Attacks, Intrusions and Defenses*. Association for Computing Machinery; 2022.
14. Chauhan U, Sharma D, Mohril S, Singh GP. A survey on energy-efficient networking and its improved security features. *Smart Computing*. CRC Press; 2021:11-17.
15. ElSawy H, Kishk MA, Alouini MS. Spatial firewalls: quarantining malware epidemics in large-scale massive wireless networks. *IEEE Commun Mag*. 2020;58(9):32-38.
16. Uçtu G, Alkan M, Doğru İA, Dörterler M. A suggested testbed to evaluate multicast network and threat prevention performance of next generation firewalls. *Future Gener Comput Syst*. 2021;124:56-67.
17. Guo L, Ye J, Du L. Cyber–physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyberattacks. *IEEE Trans Transp Electrificat*. 2020;7(2):636-648.
18. Bagheri S, Shameli-Sendi A. Dynamic firewall decomposition and composition in the cloud. *IEEE Trans Inf Forensics Secur*. 2020;15:3526-3539.
19. Radhakrishnan KK, Chinh HD, Gupta M, Panda SK, Spanos CJ. Context-aware plug-load identification toward enhanced energy efficiency in the built environment. *IEEE Trans Ind Appl*. 2020;56(6):6781-6791.
20. Chao CS, Yang SJ. A novel mechanism for anomaly removal of firewall filtering rules. *J Internet Technol*. 2020;21(4):949-957.
21. Babu TG, Jayalakshmi V. The challenges for context–oriented data accumulation with privacy preserving in wireless sensor networks. *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE; 2020:866-871.

22. Gayathri A, Prabu AV, Rajasoundaran S, et al. Cooperative and feedback based authentic routing protocol for energy efficient IoT systems. *Concurr Comput Pract Exp*. 2022;34(11):e6886.
23. Ahmadzadegan MH, Elmusrati M, Widyotriatmo A. WiMAX-based energy efficient intrusion detection system. *2013 International Conference on Robotics, Biomimetics, Intelligent Computational Systems*. IEEE; 2013:166-169.
24. Rajasoundaran S, Prabu AV, Routray S, et al. Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks. *Comput Commun*. 2022;187:71-82.
25. Pradhan D, Sahu PK, Ghonge MM, Tun HM. Security approaches to SDN-based ad hoc wireless network toward 5G communication. *Software Defined Networking for Ad Hoc Networks*. Springer, Cham; 2022:141-156.
26. Setyantoro D, Afifah V, Hasibuan RA, Aprilia N, Sari NP. The wireless computer network management security analysis. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*. 2022;7(2):105-110.
27. Luntovskyy A, Gütter D. *Highly-Distributed Systems: IoT, Robotics, Mobile Apps, Energy Efficiency, Security*. Springer Nature; 2022.
28. Demirci S, Sağıroğlu Ş. Design and evaluation of a controller for energy efficient security management and traffic routing in SDN/NFV based 5G networks. *J Faculty Eng Archit Gazi Univ*. 2022;37(1):1-5.
29. Mehic M, Duliman M, Selimovic N, Voznak M. LoRaWAN end nodes: security and energy efficiency analysis. *Alex Eng J*. 2022;61(11):8997-9009.
30. Veitch P, Macnamara C, Browne JJ. Balancing NFV performance and energy efficiency. *2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN)*. IEEE; 2022:71-75.
31. Luntovskyy A. Planning paradigms for IoT systems. *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. IEEE; 2022:1-6.
32. Kumar LS, Sultan A, Routray S, et al. Modern energy optimization approach for efficient data communication in IoT-based wireless sensor networks. *Wirel Commun Mob Comput*. 2022;2022:1-13.
33. Kumar M, Gupta O, Rani S. Firewall in underwater wireless sensor networks. *Energy-Efficient Underwater Wireless Communications and Networking*. IGI Global; 2021:120-130.
34. Kharchenko V, Kolisnyk M, Piskachova I. The research of the smart office availability model considering patches on the router firewall software. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE; 2018:169-174.
35. Khanum S, Usman M, Hussain K, Zafar R, Sher M. Energy-efficient intrusion detection system for wireless sensor network based on MUSK architecture. *High Performance Computing and Applications*. Springer; 2010:212-217.
36. Rajasoundaran S, Prabu AV, Routray S, et al. Machine learning based deep job exploration and secure transactions in virtual private cloud systems. *Comput Secur*. 2021;109:102379.
37. Benavente-Peces C. On the energy efficiency in the next generation of smart buildings—supporting technologies and techniques. *Energies*. 2019;12(22):4399.
38. Rodrigues JJ, Jabbar S, Abdallah M, Verikoukis C, Guizani M. Future communication trends toward internet of things services and applications. *IEEE Wirel Commun*. 2019;26(6):6-8.
39. Alnoman A, Carvalho GH, Anpalagan A, Woungang I. Energy efficiency on fully cloudified mobile networks: survey, challenges, and open issues. *IEEE Commun Surv Tutor*. 2017;20(2):1271-1291.
40. Latif SA, Wen FB, Iwendi C, et al. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput Commun*. 2022;181:274-283.
41. Chen Z, Sivaparthipan CB, Muthu B. IoT based smart and intelligent smart city energy optimization. *Sustain Energy Technol Assess*. 2022;49:101724.
42. Ghafari R, Kabutarkhani FH, Mansouri N. Task scheduling algorithms for energy optimization in cloud environment: a comprehensive review. *Clust Comput*. 2022;5:1-59.
43. Tabar VS, Tohidi S, Ghassemzadeh S, Siano P. Enhancing security and observability of distribution systems with optimal placement of μPMUs and firewalls. *Int J Electric Power Energy Syst*. 2022;135:107601.
44. Chobanov V, Doychev I. Cyber security impact on energy systems. *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE; 2022:1-5.
45. Haque AB, Bhushan B, Dhiman G. Conceptualizing smart city applications: requirements, architecture, security issues, and emerging trends. *Exp Syst*. 2022;39(5):e12753.
46. Tabar VS, Ghassemzadeh S, Tohidi S, Siano P. Enhancing information security of renewable smart grids by utilizing an integrated online-offline framework. *Int J Electric Power Energy Syst*. 2022;138:107954.
47. Shang Y. Integrated energy security defense monitoring software based on cloud computing. *Secur Commun Networks*. 2022;8:2022.
48. Movva SC, Nikudiya S, Basanaik VS, Edla DR, Bhukya H. Intelligent IDS: Venus Fly-trap optimization with honeypot approach for intrusion detection and prevention. *Wirel Pers Commun*. 2022;10:1-23.
49. Alkatheiri MS, Chauhdary SH, Alqarni MA. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustain Energy Technol Assess*. 2021;45:101219.
50. Tsiknas K, Taketzis D, Demertzis K, Skianis C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. *IoT*. 2021;2(1):163-186.
51. Koumaras H, Makropoulos G, Batistatos M, et al. 5G-enabled UAVs with command and control software component at the edge for supporting energy efficient opportunistic networks. *Energies*. 2021;14(5):1480.
52. Grammatikakis MD, Piperaki V, Papagrigoriou A. Multilayer NoC firewall services: case-study on e-health. *2021 15th IEEE/ACM International Symposium on Networks-on-Chip (NOCS)*. IEEE; 2021:75-81.

53. Kamoun-Abid F, Rekik M, Meddeb-Makhlouf A, Zarai F. Secure architecture for cloud/fog computing based on firewalls and controllers. *Proc Comput Sci*. 2021;192:822-833.
54. Mukhopadhyay B, Bose R, Roy S. A novel approach to load-balancing and cloud computing security using SSL in IaaS environment. *Int J*. 2020;9(2):2362-2370.
55. Pathak G, Gutierrez J, Rehman SU. Security in low powered wide area networks: opportunities for software defined network-supported solutions. *Electronics*. 2020;9(8):1195.
56. Ali ES, Hasan MK, Hassan R, et al. Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications. *Secur Commun Networks*. 2021;13:2021.
57. Han G, Zhang C, Lloret J, Shu L, Rodrigues JJPC. A mobile anchor assisted localization algorithm based on regular hexagon in wireless sensor networks. *Scientific World Journal*. 2014;2014:1-13.
58. Chen M, Qian Y, Mao S, Tang W, Yang X. Software-defined mobile networks security. *Mob Networks Appl*. 2016;21(5):729-743.
59. Rana S, Kumar N, Handa A, Shukla SK. Automated windows behavioral tracing for malware analysis. *Secur Priv*. 2022;5(6):e253.
60. Güzeltepe M, Çalkavur S. Skew-cyclic codes based public-key cryptosystem approach. *Secur Priv*. 2022;5(6):e255.
61. Gautam A, Mahajan R, Zafar S. QoS optimization in internet of medical things for sustainable management. *Cognitive Internet of Medical Things for Smart Healthcare*. Springer, Cham; 2021:163-179.
62. Zhuo M, Liu L, Zhou S, Tian Z. Survey on security issues of routing and anomaly detection for space information networks. *Sci Rep*. 2021;11(1):1-8.
63. Logeshwaran J, Shanmugasundaram N, Lloret J. L-RUBI: an efficient load-based resource utilization algorithm for bi-partite scatternet in wireless personal area networks. *Int J Commun Syst*. 2023;36(6):e5439.
64. Garcia M, Sendra S, Lloret J, Canovas A. Saving energy and improving communications using cooperative group-based wireless sensor networks. *Telecommun Syst*. 2013;52:2489-2502.
65. Xiao H, Wang L. Differential fault analysis on the lightweight block cipher plug-in plug-out. *Secur Priv*. 2023;6(3):e286.
66. Sikiru IA, Olawoyin LA, Faruk N, et al. Physical layer security using boundary technique for emerging wireless communication systems. *Secur Priv*. 2023;1:e288.
67. Manman L, Xin Q, Goswami P, Mukherjee A, Yang L. Energy-efficient dynamic clustering for IoT applications: a neural network approach. *2020 IEEE Eighth International Conference on Communications and Networking (ComNet)*. IEEE; 2020:1-7.
68. He P, Zhou Y, Qin X. A survey on energy-aware security mechanisms for the internet of things. *Fut Internet*. 2024;16(4):128.
69. Liu J. Enhancing network security through router-based firewalls: an investigation into design, effectiveness, and human factors. *Highl Sci Eng Technol*. 2024;85:724-732.
70. Durga Bhavani A, Mangla N. A review on intrusion detection approaches in resource-constrained IoT environment. *Mob Comput Sustain Inform Proc ICMCSI*. 2021;2022:171-183.
71. Abba Ari AA, Ngangmo OK, Titouna C, Thiare O, Mohamadou A, Gueroui AM. Enabling privacy and security in cloud of things: architecture, applications, security & privacy challenges. *Appl Comput Informat*. 2024;20(1/2):119-141.
72. Brahmam MG, Anand RV. VMMISD: an efficient load balancing model for virtual machine migrations via fused metaheuristics with iterative security measures and deep learning optimizations. *IEEE Access*. 2024;12:39351-39374.
73. Mahmood S, Hasan R, Yahaya NA, Hussain S, Hussain M. Evaluation of the Omni-secure firewall system in a private cloud environment. *Knowledge*. 2024;4(2):141-170.
74. Kaňuch P, Macko D. E-hip: an energy-efficient openhip-based security in internet of things networks. *Sensors*. 2019;19(22):4921.

How to cite this article: Rajasoundaran S, Sivakumar SA, Devaraju S, Pasha MJ, Lloret J. A deep experimental analysis of energy-proficient firewall policies and security practices for resource limited wireless networks. *Security and Privacy*. 2024;e450. doi: 10.1002/spy2.450