Scientific Research Publishing

Advances in Internet of Things, 2024, 14, 67-98
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

Security Concerns with IoT Routing: A Review of Attacks, Countermeasures, and Future Prospects

Ali M. A. Abuagoub

Department of Computer Engineering, College of Computer Engineering & Sciences, Prince Sattam bin Abdulaziz University, Al Kharj, Kingdom of Saudi Arabia
Email: a.abuagoub@psau.edu.sa, a.abuagoub@gmail.com

How to cite this paper: Abuagoub, A.M.A. (2024) Security Concerns with IoT Routing: A Review of Attacks, Countermeasures, and Future Prospects. *Advances in Internet of Things*, **14**, 67-98.
https://doi.org/10.4236/ait.2024.144005

Received: August 22, 2024
Accepted: October 11, 2024
Published: October 14, 2024

Abstract

Today's Internet of Things (IoT) application domains are widely distributed, which exposes them to several security risks and assaults, especially when data is being transferred between endpoints with constrained resources and the backbone network. Numerous researchers have put a lot of effort into addressing routing protocol security vulnerabilities, particularly regarding IoT RPL-based networks. Despite multiple studies on the security of IoT routing protocols, routing attacks remain a major focus of ongoing research in IoT contexts. This paper examines the different types of routing attacks, how they affect Internet of Things networks, and how to mitigate them. Then, it provides an overview of recently published work on routing threats, primarily focusing on countermeasures, highlighting noteworthy security contributions, and drawing conclusions. Consequently, it achieves the study's main objectives by summarizing intriguing current research trends in IoT routing security, pointing out knowledge gaps in this field, and suggesting directions and recommendations for future research on IoT routing security.

Keywords

IoT Routing Attacks, RPL Security, Resource Attacks, Topology Attacks, Traffic Attacks

1. Introduction

IoT routing security is a critically important factor of IoT security. Routing attacks on IoT environments can modify network parameters or performance. Security threats and attacks were categorized in [1] according to the IoT architecture layers

of transport, application, data and cloud services, physical and network protocol. In [2], the authors divided IoT attacks into a generic approach based on packet assaults, protocol attacks, and system attacks. Resources, topology, and traffic were used to categorize RPL protocol attacks in the IoT [3]-[6]. Also, physical, network, software, and data were used to classify IoT attacks and related countermeasures [7]. Common routing threats in IoT networks are categorized and briefly discussed in [8]. In this section, based on the principal targets of the assaults, IoT routing attack categories have been presented in **Figure 1**. The first category consists of resource-related attacks, which have the objective of exhausting all available bandwidth, memory, and power on the network. Attacks on topology make up the second group; they try to destabilize network topology by isolating or suboptimizing a subset of nodes. The third category consists of assaults on traffic, which aims to target network traffic by using various spoofing or dropping techniques. **Figure 1** lists the frequent attacks in each group, whereas **Table 1** briefly summarizes the primary actions and their effects for each attack.

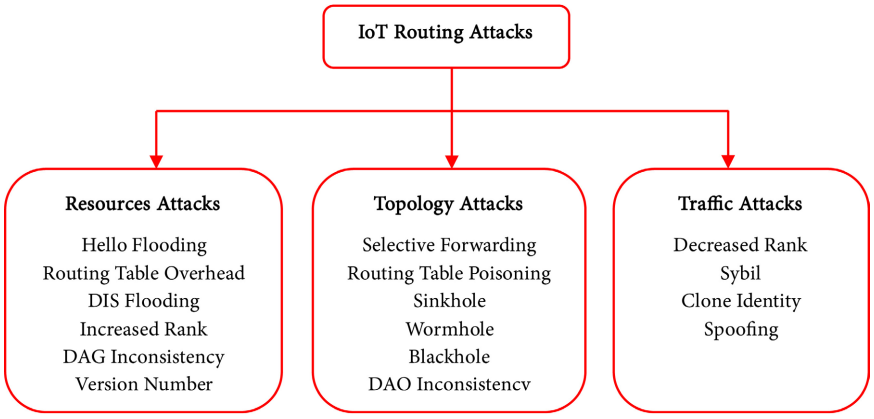

Figure 1. Categories of routing attacks.

Table 1. Common IoT routing attacks.

Attacks	Actions	Consequences
Hello flooding (HF)	An attacker sends out a flood of hello notifications, using the resources of the network and interfering with routing procedures.	Consumes bandwidth of the network and battery power of the node, resulting in a DoS attack that prevents the transmission of other legal messages.
DIS flooding (DISF)	Malicious nodes frequently broadcast DIS messages to their neighbors, who reply by resetting the DIO timers.	Increasing control overheads, lengthening end-to-end latency, and draining nodes' energy.
Increased rank (IR)	A malicious node falsely claims to be higher ranked than its actual rank to get access to more nodes in the DODAG tree.	Drains node resources, creates routing loops, slows down the network, and could result in a DoS attack.
Version number (VN)	A suspicious node initiates this attack by intentionally raising the DIO messages' advertised version number.	Raises the control message overhead, the amount of energy used, and the end-to-end delay.

Continued

Denial-of-Service (DoS)	A rogue node either generates numerous requests that clog up the available bandwidth or makes unjustified demands for extra resources.	DoS attacks make the necessary resources unavailable, preventing legitimate users from accessing the desired services.
Selective forwarding (SF)	Malicious nodes discard almost all data packets and only forward specific control messages to disrupt routing pathways.	Disrupts the flow of traffic and may cause a DoS attack.
Sinkhole (SH)	A malicious node attracts traffic on the approved route by advertising fake routing information as a trusted route toward nearby nodes, *i.e.*, a sinkhole node draws all traffic packets toward neighbors, where packets are modified or discarded.	Increases network overhead and energy use while lowering routing performance by resulting in additional attacks such as changing routing information and selective forwarding.
Wormhole (WH)	Tracking packets in a high-priority network location and establishing a tunnel for data packets to travel through to another sensing node.	Disrupts the topology of the route and causes network traffic to flow.
Blackhole (BH)	A malicious node broadcasts a bogus route to all destination nodes in a reliable way to intercept packets rather than send them. The gray hole is a special kind of blackhole attack that just loses some packets instead of intercepting all of them.	All the catching data and control packets are ejected by the blackhole node. Additionally, the blackhole attack increases DIO messages and slows down data packets.
Decreased rank (DR)	An infected node promotes a rank that is lower than its real one to capture extra traffic as a parent for other nodes.	The network traffic or energy is impacted when a rogue node is chosen as a valid parent by nearby nodes.
Sybil (SY)	Multiple nodes are faked or compromised to consume network resources; for example, Sybil nodes utilize false IDs chosen at random to confuse other nodes and impair routing performance.	Legitimate nodes are prevented from accessing network resources when resources are destroyed.
Clone identity (CI)	A rogue node can get access to a considerable portion of the network's resources by physically duplicating the identity of a genuine node. It consists of both Sybil attacks and spoofing.	By rerouting traffic from other network nodes, a cloned node could be inaccessible.
Spoofing (SP)	contains both IP spoofing and link spoofing, where a malicious node picks a random IP address and delivers a packet to the other nodes or advertises bogus links with non-neighboring nodes that may interfere with routing operations.	Causes DoS and MitM attacks or interferes with the routing of information sent.

The distributed architecture of the IoT creates distinct security challenges. A few significant aspects of IoT distribution characteristics and security challenges are emphasized as the motivation for this study. The following are a few distributed IoT characteristics:

- Massive scale: IoT networks often comprise a huge number of devices, ranging from sensors to smart appliances.
- Heterogeneity: devices in IoT networks vary widely in terms of hardware, software, and communication protocols.
- Dynamic topology: IoT networks are highly dynamic, with devices joining and departing the network continuously.

• Resource constraints: plenty of IoT devices have constrained memory, energy resources, and processing power.

• Geographical distribution: IoT devices are often spread across large geographical areas, sometimes in remote or hard-to-reach locations.

As a result of these distributed characteristics, the following unique security challenges arise:

• Scalability: securing many devices is challenging, especially when each device may have different security requirements.

• Interoperability: ensuring secure communication between heterogeneous devices using different protocols and standards.

• Data privacy: protecting sensitive data collected by IoT devices from unauthorized access and breaches.

• Physical security: IoT devices are frequently installed in unsecured environments, making them vulnerable to physical tampering.

• Resource limitations: implementing robust security measures on devices with limited resources can be difficult.

• Network security: ensuring secure data transmission over potentially insecure networks.

These characteristics and challenges necessitate innovative security solutions tailored specifically for IoT environments. The following objectives are intended to be accomplished by this article as a contribution:

• Presenting a thorough recent assessment of IoT routing attacks.

• Giving a precise picture while concentrating on the most recent mitigation and countermeasure efforts.

• Creating a roadmap for academics and researchers in this area of study.

The remaining portions of the study are presented in the following sequence: IoT routing security research is summarized in Section 2 with an emphasis on important security contributions, along with some last thoughts and observations. For the most recent research on IoT routing security, directions and technology are highlighted in Section 3. While the study is finalized by a conclusion in Section 4.

2. Related Work

Common RPL-IoT attacks were covered by [5] [6] [9]-[11], whereas [12] and [13] focused on resource-based IoT attacks and IoT layer attacks, respectively. Numerous RPL protocol attacks and their defenses were investigated in [9], where four groups of mitigation techniques were established, including secure parent selection, network monitoring, authentication/cryptography, and others. A survey was conducted on several IoT-RPL attacks, and a taxonomy of IoT-RPL attacks was developed, based on attributes and layers, research issues, difficulties, and potential future paths [5]. A review of security risks and defenses in RPL-based IoT networks was given in [10] with analysis and mapping of RPL-based IoT attacks and associated countermeasures. Attacks on IoT routing were surveyed along with

suggested defenses [6]. Several RPL attacks were reviewed, listed, examined, and differentiated from each other in [11]. To identify and eliminate resource-based assaults in the RPL network, an allied parent follow-up technique was devised, where findings showed that the suggested strategy outperformed VeRA, TRAIL, and SVELTE in the form of total latency, throughput, delivery of packets, and protected RPL topology against threats. Attacks and countermeasures were reviewed based on IoT layers, described the three-layer architectural attacks, discussed IoT security issues, and suggested solutions [13]. **Table 2** through 5 compile significant security contributions from relevant publications on IoT routing security. Each table summarizes several attacks, security measures, and final findings from relevant references.

2.1. Resources-Based Attacks

This section highlights the findings of research on attacks targeting IoT network resources. **Table 2** contains addressed attacks and potential countermeasures, as well as concluding observations.

Table 2. Summary of research on IoT routing resources-based attacks.

Ref.	Attacks	Key Security Contributions	Concluding Remarks/Arguments
[14]	Hello Flooding	Defenses and link flooding attacks (LFAs) were modeled [14].	The suggested model greatly increased striking precision at the expense of a modest strike efficiency decrease [14].
[15]		A gated-recurrent-unit (GRU) approach was devised depending on deep-learning for discovering and thwarting hello-flooding attacks on RPL-IoT networks [15].	In comparison to SVM and LR approaches, simulation results verified the claimed and predicted source efficiency and IoT security from the GRU model [15].
[16]		A rider-optimization algorithm based on bypass-linked-attacker-update (BAU-ROA) was developed for hello flooding [16].	According to an experimental study, the BAU-ROA was more effective than the D-DHOA, DHOA, and WOA in identifying and avoiding hello-flooding attacks [16].
[17]		Provided a thorough analysis of the RPL's susceptibility to the HF attack in mobile settings [17].	Evaluated the performance of M-RPL-Based-IoT-Network [17].
[18]	DIS Flooding	A novel secure RPL protocol mechanism was proposed for mitigating DIS flooding attacks and preventing insider and outsider attacks [18].	The suggested system could improve network lifespan, throughput, and packet delivery while reducing total delays, loss of packets, energy usage, and controlling message's overhead, according to simulation results [18].
[19]		It was suggested that a Maximum Response Code (RPL-MRC) be used in IoT-LLNs to mitigate DIS Multicast attacks [19].	The RPL-MRC mechanism's effectiveness for lowering energy usage and overhead was shown by simulation results [19].
[20]		A secure scheme was proposed for mitigating DIS Flooding (DISF) attacks in 6LoWPAN networks based on RPL [20].	According to experimental findings, the Secure RPL, as compared to regular RPL, detected, and eliminated DIS-flooding attacks quickly and efficiently without incurring appreciable overheads [20].

Continued

[21]	DIS Flooding	ML-based methods were used for detecting IoT DISF attacks [21].	Evaluation findings demonstrated that the LR had greater attack detection accuracy [21].
[22]		The influence of DIS-flooding was analyzed for 6LoWPAN RPL-based [22].	The analysis's findings demonstrated that increasing DIS flooding attackers and deployment locations produced significant negative impacts on end-to-end delaying, PDR, and power usage [22].
[23]	Version Number	It was suggested to use a Machine Learning - Light Gradient Boosting Machine (ML-LGBM) to recognize RPL Version Number (VN) attacks [23].	According to experimental findings, the ML-LGBM model has advantages in terms of false-positive, true-negative, F-score, precision, and accuracy rates [23].
[24]		A framework was proposed for determining version-number attacks in IoT [24].	Mechanisms for spotting the attack and locating suspicious nodes launching version number attacks were presented [24].
[25]		The IoT-RPL-based network performance was evaluated under VN attacks [25].	In the event of version attacks, the network's performance was analyzed with a focus on PDR, power usage, and latency [25].
[26]		A Q-learning strategy was proposed for detecting RPL-based IoT version number attacks [26].	The findings demonstrated that the QSec-RPL technique detected malicious nodes reasonably accurately while incurring less node overhead [26].
[27]		Surveyed version number detection mechanisms [27].	Analyzed gaps and suggested future research directions [27].
[28]	Denial-of-Service	A lightweight-trust-based security system was proposed to protect RPL from D-DoS attacks [28].	The suggested system performed well regarding detection ratio, delaying, delivery, and throughput, according to the simulations' outcomes [28].
[29]		An optimized trustable route node convention (OTRNC) approach was proposed for securing IoT-MANET [29].	In comparison to MQARP and SCGF, the OTRNC enhanced packet delivery, detection effectiveness, network longevity, and packet integrity [29].
[30]		A secure-link-state-routing protocol (SLSRP) was proposed for the transfer of information in IoT [30].	According to simulation results, the SLSRP outperformed OSPF in terms of timeliness and dynamic adaptability in the presence of IoT DoS attacks [30].
[31]		The impacts of copycat attacks on RPL IoT were investigated [31].	According to experimental findings, copycat attacks can substantially decrease the performance of networks concerning packet arrival, end-to-end latency, and energy use [31].
[32]		An ensemble feature selection (FS) approach was provided to identify RPL networks' DDoS attacks [32].	Support vector machine (SVM) and three bio-inspired algorithms were used in the ensemble FS to discover and diagnose DDoS-flooding attacks on RPL networks [32].
[33]	Denial-of-Service	A secure-trust-aware-routing (ST2A) protocol was developed to provide a route that is secure and dependable in WSN [33].	By comparison to the LEACH and EMPIRE algorithms, the simulation results verified the feasibility of the ST2A for improving network lifetime and data delivery [33].
[34]		A DDoS flooding attack detection framework was designed for intelligent transportation systems (ITS) [34].	The effects of DDoS flooding attacks on ITS were examined together with the usefulness of the suggested framework for detection using reinforcement learning [34].

Continued

[35]		It was suggested to use deep learning to identify DoS attacks [35].	When compared to the most recent approach, the proposed strategy has an accurate detection and the lowest rate of false positives [35].
[36]		An SDN and ML-based secure routing algorithm has been presented for the IoT (SRAIOT) [36].	The SRAIOT enhances attack detection and routing efficiency [36].
[37]	Hello/DIS Flooding	A DFA-RPL method was proposed for securing the data gathered by IoT devices [37].	In comparison to IRAD and REATO methods, simulation results demonstrated the DFA-RPL approach's superiority in the false negative, false positive, detection, and packet delivery rates [37].
[38]	Version Number, DDoS	A routing protocol called GSDO-RPL which is geographic-location-based, opportunistic, and secure-dynamic was introduced over RPL [38].	According to simulation results, the GSDO-RPL managed security, scalability, and mobility better than RPL [38].

2.2. Topology-Based Attacks

This section investigates topological attacks in IoT network research. Table 3 summarizes the addressed attacks and solutions, as well as the conclusions, where it can be observed that the Sinkhole and Blackhole attacks are examined by a remarkably large number of researchers.

Table 3. Summary of research on IoT routing topology-based attacks.

Ref.	Attacks	Key Security Contributions	Concluding Remarks/Arguments
[39]	Selective Forward	A novel detection technique based on artificial intelligence has been presented for preventing selective forwarding attacks in IoT based on RPL [39].	Results collected demonstrated the success of the suggested method regarding packet delivery, packet delay, and attack detection during selective forwarding [39].
[40]		A trust-based defense approach was suggested to identify and prevent selective forwarding attacks [40].	The findings demonstrated that the suggested method provided good detection accuracy at the cost of slightly more energy usage [40].
[41]		The impact of Selective Forwarding (SF) attacks in IoT was evaluated [41].	The findings demonstrated that the selective forwarding attack dropped both latency and PDR [41].
[42]	Sinkhole	A random forest trust (RFTRUST) prototype was designed to handle the sinkhole attack in RPL-based IoT environments [42].	As compared to the InDReS, INTI, and SoS-RPL prototypes, simulation results revealed that RFTrust has a high PDR and throughput, a low average delay and energy consumption, high accuracy, a low false-negative, and a low false-positive rate [42].
[43]		A SoS-RPL approach was suggested. for detecting sinkhole attacks in IoT [43].	According to simulation results, SoS-RPL outperformed SecTrust-RPL, Fuzzy-IoT, IRAD, and REATO concerning throughput, false-positive and false-negative detection rates, packet loss, and packet delivery [43].
[44]		A distributed IDS was proposed for discovering sinkhole attacks in RPL-based IoT networks [44].	Compared to support vector machines (SVM) and Bayesian classifier, the decision tree (DT) technique had the highest level of precision [44].

Continued

[45]	Sinkhole	Surveyed sinkhole attacks [45].	Attacks using sinkholes are frequently used as a lead-up to more destructive ones [45].
[46]		An effective algorithm was provided for detecting sinkhole attacks in IoT-based WSNs [46].	The findings demonstrated that, at various distances from BS, the suggested approach achieved good accuracy in sinkhole detection [46].
[47]		An intrusion detection algorithm was suggested for protecting IoT devices from sinkhole attacks [47].	The simulation results proved that the suggested framework outperformed earlier approaches regarding the accuracy of identification and the rate of false positives [47].
[48]		A knowledge-based specification rule was deployed to improve the IoT sinkhole attack detection rate [48].	The findings demonstrated that, in comparison to the INTI approach, the suggested method generally gave a greater sinkhole attack detection ratio [48].
[49]		A review of sinkhole attacks in RPL was given [49].	An overview of sinkhole attacks in RPL-based IoT was provided, along with security concerns [49].
[50]	Sinkhole	An approach for detecting sinkhole attacks in the edge-based Internet of Things (SAD-EIoT) has been developed [50].	According to the analysis of the findings, the SAD-EIoT outperformed related schemes concerning the false positives' number and the discovery's rate [50].
[51]		A reputable trust-based intrusion detection system (DSTIDS) with a direct neighbor sink was introduced to mitigate sinkhole attack effects [51].	According to simulation results, the DSTIDS performed well in terms of detection rate, PDR, FPR, and FNR [51].
[52]	Sinkhole, Selective forw	The performance of RPL was evaluated under sinkhole and selective forwarding attacks [52].	Comparison and evaluation scenarios revealed that the affected nodes consumed higher power [52].
[53]	Blackhole, Selective Forward	A security strategy was devised to recognize and prevent selective forwarding and blackhole attacks in medical IoT-WSN [53].	The investigation proved that, in comparison to DHOA and WOA, the D-DHOA produced better outcomes [53]. The outcomes
[54]		An anomaly for detecting 3 (AD3) RPL (RPLAD3) attacks was proposed in WSN-based IoT [54].	Showed that the RPLAD3 outperformed the RPL in thwarting attacks with significant precision and a true +ve ratio while consuming less energy and power. Additionally, it substantially raises the rate of packet delivery rate and brings the false +ve to zero ratio [54].
[55]	Wormhole	RHE2WADI was suggested as a hop-count-based energy-efficient and RSSI solution for discovering IoT wormhole attacks [55].	According to the results, the RHE2WADI outperformed existing wormhole IDSs in terms of energy consumption, TPR, FPR, propagation delay, MCC, accuracy, and F1 score [55].
[56]		A review of wormhole attacks was presented for IoT/WSN [56].	The study of the data revealed that the IoT has a stronger detection capability than the WSN [56].
[57]		An energy-optimized security (ESWI) technique was developed for identifying wormhole attacks in WSNs IoT-based [57].	The simulation results demonstrated that, in comparison to other proposed detection techniques, the ESWI achieved a high recognition rate, enhanced throughput, increased delivery ratio, reduced power use, and decreased latency [57].

Continued

[58]	Wormhole	TOPSIS and hashing techniques were used in a Sec-IoT method that was developed to counter wormhole attacks [58].	The outcomes of the simulation demonstrated that the proposed technique performed better in PDR, PLR, and throughput than HRCA and HBC methods [58].
[59]		Invalidating tunneling attacks in IoT WSNs was done using ML techniques [59].	The ML approaches enhanced PDR, delay, and network lifetime [59].
[60]		Subjective Logical Framework-RPL(SLF-RPL) was proposed [60].	SLF-RPL outperformed PCL-RPL [60].
[61]	Blackhole	A hybrid optimization algorithm was used to prevent blackhole attacks in IoT-based WSNs [61].	Performance evaluations showed that the HOA-IoT-WSN approach performed much better than the LWTS, HHH-SS, and ESR methods [61].
[62]		A security safeguard was introduced to protect RPL-based WSNs from black hole attacks [62].	The mechanism has a high true positive rate, decreased packet loss, and great accuracy for detecting black holes [62].
[63]		For black hole and packet falsification attacks, an Opportunistic IoT (OppIoT) with a green forwarding ratio and RSA-based (GFRSA) secure routing protocol was developed [63].	According to simulations, the GFRSA offered message security while saving energy and outperforming the LPRF-MC and RSASec concerning packet delivery and residual node energy [63].
[64]		The DPBHA method, which detects and prevents black hole attacks, was suggested for VANETs [64].	The suggested DPBHA performed better than the AODV, SAODV, and IDBA regarding packet delivery, throughput, routing overhead, detection rate and end-to-end delay, according to presented results [64].
[65]		A honeypot agent-based scheme with long-short-term memory (HPAS-LSTM) was used for detecting black hole attacks on MANET [65].	According to the results of the simulation, the HPAS-LSTM performed better than the HPAS-Bi-LSTM, HPAS-RNN, and HPAS-ReNN in the context of throughput, packet loss, delivery, and delay [65].
[66]	Blackhole	A security technique based on trust support vector regression (TSVR) was developed to prevent and detect black hole attacks on the Internet of Battlefield Things (IoBT) [66].	According to the simulation study, the TSVR outperformed RPL and comparable present mechanisms [66].
[67]		For identifying and isolating black hole attacks, a control layer-based trust mechanism (CTrust-RPL) was proposed to allow secure routing in RPL-based IoT systems [67].	The findings revealed that, in comparison to Sectrust, the CTrust-RPL performed better in identifying and isolating blackhole attacks [67].
[68]		A technique for detecting black hole attacks in IOT was suggested [68].	The network's performance was improved, and power consumption was decreased through black hole node detection and removal [68].
[69]		An ad-hoc on-demand distance vector (AODV) routing protocol for collaborative black hole attacks (CBHA-AODV) was suggested [69].	According to the findings, the CBHA-AODV protected against cooperative black hole attacks in the IoT construction environment [69].

Continued

[70]	Blackhole	A svBLOCK scheme was presented for dealing with blackhole attacks [70].	The findings showed that the svBLOCK outperformed the SVELTE in TPR, FPR, and PDR [70].
[71]		AODV routing protocol was used to examine the performance of the ad-hoc IoT network under blackhole attacks [71].	Investigations included the evaluation of protocol vulnerability and assault damage analysis for digital forensics [71].
[72]	Blackhole, Wormhole	Assessing the effects of wormhole and blackhole attacks on the MANET cloud-equipped IoT network used for agriculture surveillance fields [72].	Jitter-sum, end-to-end delay, packet delivery ratio, and throughput were used for evaluating the results using NS-3, which can be helpful for IoT smart agriculture [72].

2.3. Traffic-Based Attacks

This section summarizes the research on traffic-based attacks in IoT networks. Table 4 highlights the assaults addressed, and remedies proposed, as well as the ultimate conclusions. It can be noticed that Sybil's attacks were considered by a significant portion of researchers.

Table 4. Summary of research on IoT routing traffic-based attacks.

Ref.	Attacks	Key Security Contributions	Concluding Remarks/Arguments
[73]	Decreased Rank	S-MODEST, a secure RPL based on DEmpster Shaffer Theory and non-cooperative game MODels, has been suggested by IoT researchers [73].	Simulation findings showed that the S-MODEST outperforms the existing SecTrust concerning throughput, detection accuracy, and energy usage [73].
[74]		For identifying decreasing rank attacks in IoT networks based on RPL, an artificial neural network (ANN) scheme was suggested [74].	The ANN performed better than earlier techniques for precision, recall, and F-score metrics as well as showed promising results for AUC-ROC, false positive rate, precision, and accuracy [74].
[75]		Investigated hybrid rank (DR, WP) attack [75].	Mitigated DR and WP attacks (HRA) [75].
[76]	Sybil	A novel decentralized countermeasure was devised for recognizing sybil attacks in IoT-RPL networks [76].	The suggested solution was evaluated regarding, accuracy of attack detection, average power usage, attack isolation time, average packet delivery ratio, and control message overhead [76].
[77]		An artificial bee colony with a lightweight intrusion detection mechanism was proposed for mitigating mobile RPL Sybil attacks [77].	The findings demonstrated that the suggested lightweight intrusion detection algorithm performed better than expected in the context of accuracy, specificity, and sensitivity [77].
[78]		A Gini index-based countermeasure (GINI) was proposed for identifying and reducing sybil attacks in RPL [78].	According to simulation results, the GINI outperformed SecRPL and two-step detection in terms of detection rate and delay as well as energy consumption [78].
[79]		A Lightweight, and Efficient Trust-based Mechanism for IoT (LETM-IoT) was suggested for Sybil's attacks [79].	The experimental results demonstrated that LETM-IoT performed better than standard RPL and state-of-the-art approaches for average packet-delivery ratio, memory utilization, true-positive ratio, and energy consumption [79].
[80]		A countermeasures review was conducted on the Sybil attacks in IoT-based WSNs [80].	RSSI, encryption, trust, and AI were mentioned as modern defenses against Sybil attacks [80].

Continued

[81]	Sybil	IoT Sybil attacks were detected and prevented using the received signal strength indicator (RSSI), the lightweight encryption algorithm (LEA), and the Caesar cipher algorithm (CCA) [81].	According to simulation findings, the RSSI-LEA-AODV method offered reliable network performance in the presence of Sybil attacks [81].
[82]		Machine learning approaches were proposed for detecting attacks in IoT-based SN [82].	Simulation findings demonstrated that ML approaches (LR, NB, and RF) provide greater detection accuracy than conventional techniques [82].
[83]		For recognizing Sybil attacks in RPL-based IoT networks, a trust-based hybrid cooperative RPL (THC-RPL) framework was developed [83].	The results of the performance evaluation revealed that the THC-RPL performed better than the best in terms of attack detection, PLR, and energy usage [83].
[84]	Clone Identity	A DNN was proposed for identifying RPL attacks caused by clone ID [84].	Because of their signature-based detecting methods, IDS, IPS, and SIEM are becoming insufficient for correctly handling innovative security occurrences [84].
[85]		A routing protocol for energy efficient networks (RPEEN) was proposed for detecting clone attacks in IoT-based smart health [85].	Considering the simulation's results, the RPEEN outperformed the HMLC in terms of latency, error rate, energy efficiency, throughput, and residual energy [85].
[86]	Spoofing	A secure routing based on cryptography and cross-layer (CLCSR) approach was proposed for preventing attack, protecting user safety, and securing data transfer [86].	Based on the outcomes of the simulation, the CLCSR protocol outperformed HSR and ESR in the context of cryptography time, routing overhead, packet delivery, energy use, and throughput [86].
[87]		For a WSN-based IoT context, a Routing Protocol based on Multihop Dynamic Clustering for Optimal Privacy (OP-MDCRP) with Encryption-Key Provisioning Method Integrated Elliptic Curve (ECIES-KPM) was developed to increase data privacy and routing effectiveness [87].	According to an experimental comparison, the OP-MDCRP technique performed better than ESR and LEACH-MAC concerning, energy consumption, end-to-end delay, packet delivery, network overhead, and longevity [87].
[88]		A cluster head, key authentication, and secure routing were introduced for IoT-based WSNs [88].	Evaluation of performance showed that the devised technique outperforms SQEER and STEAR regarding throughput. It also outperforms LEACH-MAC, ESR, and OP-MDCRP in terms of energy use, network lifetime, overhead, packet delivery, and end-to-end delay [88].

Additionally, a scalable and secure routing protocol with attestation (SARP) was proposed for IoT-based networks, where the simulation results demonstrated SARP's effectiveness concerning data integrity, communication security, packet delivery ratio, network overheads, and power usage in the occurrence of various IoT attacks [89]. A honeybee crossover mutated marriage (CM-MH) technique and enhanced blowfish algorithm were developed for determining the best path and safeguarding transmission, and the evaluation findings demonstrated that the developed approach outperformed several techniques, including PSO, FF, GA, and MHBO models [90]. Comparisons were made between several RPL-based intrusion detection systems [91] [92], and guidance was presented for upcoming

research and design requirements for contemporary RPL-IDS [91]. An enhanced RPL (ERPL) protocol was proposed for protecting IoT-based LLNs from worst-parent attacks, where the results of the comparison proved that the ERPL performed superior to the RPL concerning energy use, network overhead, convergence, and packet delivery [93]. Mitigating security mechanisms were proposed for reducing the effect of DAO attacks on the RPL, and simulation findings demonstrated that the devised techniques restored the ideal network productivity in the context of consuming energy, latency, packet delivery, and overheads [94]. A sequential-convex-estimation-optimization (SCEO) method was developed with a swift-privacy-rate-optimization mechanism, to increase the physical layer's security, and according to the findings of the investigation, the SCEO algorithm increased convergence in the transmission while achieving ideal performance [95].

2.4. Multiple Sets of IoT Routing Attacks

This section has examined research on various types of IoT routing attacks. **Table 5** illustrates the addressed different kinds of attacks, proposed remedies, and conclusion findings.

Table 5. Summary of research on different types of IoT routing attacks.

Ref.	Attacks	Key security contributions	Concluding remarks/arguments
[3]	IR, DR	A holistic framework was introduced for routing attacks anticipating in RPL-based IoT-LLNs [3].	Three different forms of attacks, including resource, topological, and traffic attacks, have been successfully tested using the proposed system [3].
[4]		A review of rank attacks was provided with some mitigating techniques [4].	Research articles on rank attack security have been compared and discussed [4].
[96]		An objective function based on echelon metrics (EMBOF) was developed above the RPL to identify and isolate rank attacks [96].	According to experimental findings, the EMBOF-RPL outperformed SVELTE, SBIDS, and SecTrust in terms of attack isolation and detection, power usage, end-to-end delay, memory usage, and packet delivery [96].
[97]		A secure RPL technique based on moth-flame optimization (MFO-RPL) was developed to improve routing and identifying rank attacks [97].	According to simulation results under various conditions, the MFO-RPL achieves less convergence time, rank switching, and packet loss than comparator techniques [97].
[98]		An enhanced rank attack detection (E-RAD) method was proposed to identify and isolate rank attacks [98].	The findings demonstrated that the E-RAD improved detection precision, end-to-end delay, and PDR with tolerable control overhead [98].
[99]		An energy-efficient lightweight mechanism was proposed for isolating and mitigating rank attacks in RPL-based IoT [99].	The suggested algorithm performed more accurately in grid-centered topology and consumed less energy in random topology when compared to existing algorithms [99].

Continued

[100]	WH, SP	A secure hybrid routing was proposed for discovering and preventing adversaries in IoT-based WSNs [100].	The SHR demonstrated a higher attack identification ratio for IP spoofing and wormhole attacks when compared to OLSR, DSDV, AOMDV, and TARCS [100].
[101]		A chaotic bumble bee mating optimization with a trust sensing model (CBBMO-TSM) was developed for securing IoT data transmission [101].	Comparing the CBBMOR-TSM model to the MCTAR-IOT, OSEAP_IOT, and TRM_IOT strategies, on average, the PDR and PLR were greater for the CBBMOR-TSM model [101].
[102]	BH, DoS	Deep reinforcement learning was used to build a secure routing protocol with quality-of-service awareness (DQSP) for SDN-IoT [102].	Simulation studies indicated that the DQSP outperformed the OSPF routing protocol under the gray hole and DDoS attacks, demonstrating good convergence and high effectiveness [102].
[103]		ML-based approaches were implemented for detecting IoT attacks [103].	In comparison to the decision forest tree regression, decision tree jungle, and boosted decision tree regression, the ML-based method achieved greater accuracy in identifying IoT attacks [103].
[104]	SP, DoS	A CoSec-RPL was proposed as an intrusion detection system for mitigating the consequences of non-spoofing copycat assaults on the performance of networks [104].	In comparison to the traditional RPL protocol, testing results showed that the CoSec-RPL efficiently identifies and prevents non-spoofing copycat attacks in both mobile and static network settings without significantly increasing node overheads [104].
[105]	DoS, WH, GH	A LIDOR (Lightweight-DoS-Resilient) protocol was proposed for protecting IoT-systems from well-known packet-dropping attacks [105].	Experimental findings revealed that the LIDOR improved reliability under DoS attacks and it was resilient under replay and wormhole attacks [105].
[106]	BH, DR	For secure IoT routing, a trust- and mobility-based protocol was suggested [106].	According to the evaluation's findings, SMTrust performed better than MRHOF, SecTrust, DCTM, and MRTS concerning packet loss, throughput, and stability [106].
[107]		A security, mobility, and trust-based (SMTrust) approach was suggested for RPL attacks in IoT [107].	SMTrust outperformed SecTrust, DCTM, MRTS, and MRHOF, according to simulation testing [107].
[108]	SY, WH	A localization with early detection (LiDL) method was proposed for Sybil and wormhole attacks [108].	The outcomes showed that the LiDL was feasible in terms of TPR, PLR, memory usage, detection time, and network overhead [108].
[109]	VN, IR, DR	A novel blockchain-based framework was proposed for protecting IoT-LLNs against routing threats [109].	The suggested system produced alerts in real-time to identify the compromised sensor nodes [109].
[110]	HF, DR, VN	An artificial intelligence-aided machine learning approach (AIEMLA) was proposed to avoid routing assaults in IoT [110].	Hello flooding, rank decreased, and version number attacks were all accurately identified by the AIEMLA concurrently or separately [110].
[111]	IR, DR, DISF	An intrusion detection system based on gaming models anomalous (GAIDS) was developed for securing RPL [111].	Based on simulation outcomes the proposed GAIDS-RPL surpasses the existing FSM-RPL in terms of detection accuracy and throughput [111].

Continued

[112]	SF, WH, BB	A secured MAC-based cross-layer routing mechanism for IoT Networks [112].	Comparing the suggested model to other systems CM-LA, LA, CS, FF, PSO, and GA, secure routing was achieved with little risk [112].
[113]	IR, DR, VN	A routing protocol based on secured RPL (SRPL-RP) was proposed for detecting, mitigating, and protecting IoT from version-number and rank attacks [113].	In comparison to normal RPL, RPL-Shield, and sink-based intrusion detection systems (SBIDS) under various network topologies, analysis findings illustrated that the SRPL-RP achieved substantial advancements concerning average energy usage, control message value, and packet delivery ratio [113].
[114]	BH, SF, WH	The efficiency of RPL security mechanisms was assessed against common IoT routing attacks [114].	According to analysis, the RPL's built-in secure mode can successfully counteract blackhole and selective-forwarding attacks [114].
[115]	DoS, MITM, Flooding	A Lightweight Compressed host identity protocol Diet EXchange (LC-DEX) was designed for constrained IoT device security [115].	The findings illustrated that the suggested technique protected communication for WSN IoT-based systems while consuming little energy [115].
[116]	IR, DR, VN	IoT-based RPL routing attacks were reviewed [116].	A thorough analysis of rank and version number attacks and their defenses was given [116].
[117]	BH, SF, WH	A Self Improved Sea Lion Optimization (SI-SLnO) algorithm was suggested for the best route selection with rule-based attack detection in IoT [117].	In comparison to PSO, GA, CS, CM-LA, FF, and LA, analysis with various numbers of infected devices showed that the proposed model got superior outcomes with the least amount of expense [117].
[118]	HF, DR, VN	IoT RPL-based routing attacks were investigated [118].	All IoT attacks are found to increase network traffic, alter the DODAG tree, and hence increase power consumption [118].
[119]	IR, DR, BH	A MRTS (Metric-based-RPL-Trustworthiness- Scheme) was designed for securing routing topology construction [119].	According to simulation results, the MRTS is more effective than MRHOF and SecTrust under blackhole and rank attacks concerning throughput, rank changes, energy utilization, and packet delivery [119].
[120]	SH, WH, SY	A TBEERP (Trust-Based-Energy-Efficient-Routing-Protocol) was proposed for IoT–based sensor networks [120].	According to experimental findings, the TBEERP performed better than EAMR, ETLHCM, ABC-SD, and FUCARH regarding network longevity, packet delay, energy consumption, and throughput [120].
[121]	HF, DR, VN	An early-stage detection based on deep learning (DL-ESD) was proposed for discovering version number, decreased rank, and hello flooding attacks [121].	The outcomes showed that the DL-ESD scheme outperformed LR, KNN, SVM, NB, and MLP concerning F1 score, prediction, precision, accuracy, and recall [121].
[122]	SH, IR, DR	The SVELTE algorithm was modified for detecting sinkhole and rank attacks [122].	The findings demonstrated that the redesigned SVELTE offered superior TPR, FPR, and energy using [122].
[123]	IR, DR, WH	A multiclass classification-based ML gradient boosting machine-based (MC-MLGBM) algorithm was developed for IoT RPL attacks [123].	The outcomes showed that the MC-MLGBM offered superior precision, recall, and accuracy compared to RA and WHA [123].

Continued

[124]	SH, HF, DoS	A DQNSec routing approach was proposed for OppIoT [124].	According to simulation results, DQNSec is more effective than CAML, RLProph, MLProph, and RFCSec [124].
[125]	SH, SF, SY	Developed a TIDSRPL (Trust-based-Intrusion-Detection-System-RPL) [125].	Analysis results showed that the TIDSRPL outperformed MRHOF-RPL [125].
[126]	HF, VN, SH, BH	A framework was proposed to identify the existence of security risks in IoT-IIoT networks based on RPL [126].	The effectiveness of the suggested framework was assessed regarding the true+ve rate, false+ve rate, packet delivery rate, and end-to-end delay [126].
[127]	IR, DR, BH, DISF	A security RPL framework was proposed for IoT networks (SRF-IoT) [127].	According to simulation analyses, the implementation of the framework is more successful than not deploying it concerning enhancing packet delivery, minimizing packet drops, and reducing the number of parent switches [127].
[128]	IR, DR, VN, BH, SY	A machine-learning method was used for detecting combined IoT attacks [128].	Results that were recorded showed that the machine learning approach correctly identified all combination attacks [128].
[129]	DR, SH, BH, SF, HF, VN	An intrusion detection system was developed using machine learning for recognizing common RPL routing attacks [129].	Decision trees, k-nearest neighbors, and random forests all outperformed other methods in experiments using 5-fold cross-validation, but logistic regression, MLP, Naive Bayes, and deep learning, performed worse [129].
[130]	SY, IR, DR, BH	A fuzzy, dynamic, and trust method based on RPL (FDTM-RPL) was suggested for defending against IoT threats [130].	The evaluation's findings demonstrated that, when compared to the RPL protocol standard, the FDTM-RPL offered considerable reductions in the end-to-end delay, packet loss, and average number of parent changes [130].
[131]	IR, DR, SY, SH	A trusted framework based on RPL for multi-mobile agent-based (MMTM-RPL) was proposed for protecting IoT-based wireless sensor networks from internal attacks [131].	According to experimental findings, the MMTM-RPL outperformed the DSH-RPL, RPL-MRC, RBAM-IoT, and DCTM-RPL in terms of Rank, Sybil, and Sinkhole attack mitigation, energy and message overhead reduction, increased network lifetime, and detection rate [131].
[132]	HF, DoS, SF, BH, SY	A secure and adaptive multipath RPL (SAMP-RPL) has been proposed for improving reliability and security in heterogeneous IoT-connected LLNs [132].	Results of the evaluation demonstrated the SAMP-RPL's superiority over random secure multipath RPL, continuous, and loss-driven in terms of boosting reliability and security at a reasonable cost [132].
[133]	DIOS Suppression, DISF, SF, BH, SY, SH	Machine learning approaches were presented to spot risks in RPL-based IoT networks [133].	Several machine learning approaches have been used, such as decision trees (DT), adaboost (AdB), k-nearest-neighbors (KNN), logistic regression (LR), random forest (RF), gaussian-naïve-Bayes (GNB), and multilayer perceptron (MLP) [133].
[134]	SY, Flooding, BH	It was suggested to use a secure RPL (Sec-RPL) to manage congestion [134].	According to the simulation results, the Sec-RPL outperformed the control system according to PDR, PLR, delay, energy consumption, and load balance [134].

Continued

[135]	VN, DDoS, BH, GH, DAO, Flooding	An IDS was developed for IoT-RPL networks [135].	The evaluation's findings demonstrated that the IDS detected attacks with a high degree of accuracy while only slightly increasing power usage [135].
[136]	IR, DR, SF, WH, DoS	Multiple intrusion detections for IoT networks based on RPL have been proposed [136].	According to simulation results, machine learning approaches can be used to detect multiple intrusions efficiently [136].
[137]	DR, BH, SH, SF	A fuzzy k-NN classifier was proposed for detecting RPL attacks in IoT networks [137].	According to the simulation findings, the suggested RPLML-IDS performed better than both Logistic Regression and the k-NN classifier [137].
[138]	IR, DR, VN, Worst Parent, Replay	A presentation was made on an experimental investigation of RPL routing attacks that took into consideration simple to complicated attack scenarios [138].	According to the findings, even simple attack scenarios caused the networks to noticeably degrade QoS performance and network stability, as well as noticeably increase control traffic overhead and energy usage [138].
[139]	DISF, IR, DR, WH	A hybrid deep learning-based IDS was proposed for RPL IoT Networksb [139].	According to the findings, multi-class attacks had a detection accuracy rate of 98%, while pre-trained attacks had an average accuracy rate of 95% [139].
[140]	SH, SF, SY, BH, HF, DDoS, WH, IR, DR, VN	To identify routing attacks, A system for hybrid intrusion detection (HIDS) was proposed, which incorporates two classifiers one-class support vector machine and a decision tree [140].	With greater detection and fewer false +ve rates, the outcomes demonstrated that the HIDS outperformed both SIDS and AIDS techniques [140].
[141]	WH, SY, SF, BH, DDoS, SP	Network management utilizing machine learning was provided together with an analysis of security vulnerabilities in the WSN-IoT [141].	A thorough analysis of the characteristics and attributes of WSN-IoT for low-powered IoT mechanisms was given [141].
[142]	BH, Flooding, WH, SH, SF	A fuzzy logic-based secure hierarchical routing scheme employing the firefly algorithm (FSRF) is presented to detect and stop routing attacks in IoT-based healthcare systems [142].	Comparing the FSRF to E-BEENISH and EEMSR increases network lifetime and node storage of energy. But in terms of security, FSRF is less strong than EEMSR, and its PDR has been slightly decreased [142].
[143]	HF, CI, SF, BH, SY, SH	Provides an overview of IoT network security [143].	ML-approaches for identifying IoT network layer attacks are provided [143].

The distributions of articles among IoT routing attacks are quantitatively presented in **Figure 2**, where the attacks can be arranged in decreasing order of publication as follows: Blackhole, Decreased rank, Increased rank, Sinkhole, DoS, Sybil, Wormhole, Selective forwarding, Version number, Hello flooding, Spoofing, and Clone identity. **Figure 3** depicts the distribution of each IoT routing attack in recent years.

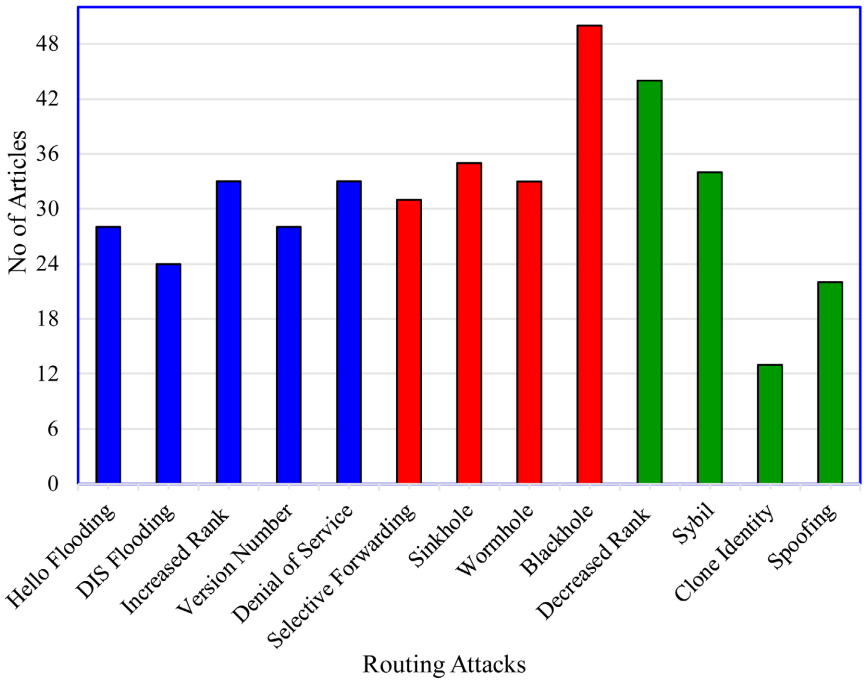

Figure 2. Distribution of the existing research on IoT attacks.

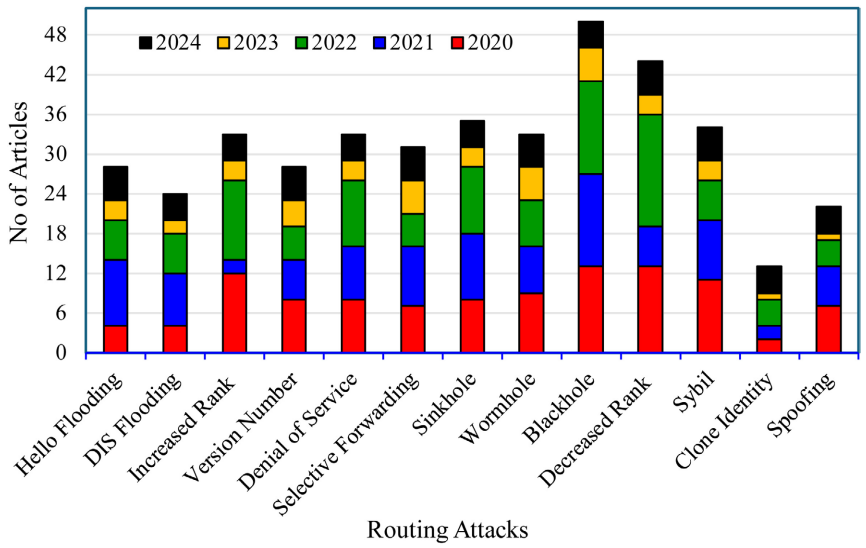

Figure 3. Frequency of the IoT attacks' studies in recent years.

2.5. Limitations and Shortcomings

This subsection briefly discusses common limitations and shortcomings on typical examples from most recent studies. The following summarizes the key components:

- Limited scope of attack scenarios: several studies have been designed for certain types of attacks, potentially overlooking different kinds of attacks that could affect RPL-based IoT networks, and may not be easily adaptable to target other types of RPL network attacks [25] [26] [54] [58] [60] [75] [125] [138]-[140] [142] [144]. The studies in [25] [26] primarily focus on version number attacks. In [54]

the study primarily addresses selective forwarding, grayhole, and blackhole attacks. The solutions in [58] [60] are specifically designed for wormhole attacks. Hybrid rank attacks are addressed in [75]. The study in [138] primarily addresses simple and complex routing attacks.

• Scalability concerns: a number of studies do not extensively address the scalability of the proposed solutions in larger networks with a higher number of nodes [25] [26] [54] [58] [60] [75] [125] [138] [139] [142]. In [26] the study does not thoroughly investigate how the proposed solution scales with increasing nodes and varying network sizes. The SMTrust shows improved performance [106], but its scalability in extremely large networks with thousands of devices remains untested.

• Computational complexity: some proposed solutions can be computationally intensive, which might not be appropriate for IoT devices with limited resources [26] [58] [60] [125] [139] [140] [142] [144]. Such as the implementation of the Q-Learning [26], the TOPSIS decision-making and hash-based cryptography [58], the subjective logical framework [60], the hybrid deep learning approach [139], the fuzzy logic and the firefly algorithm [142], and the Swan Intelligent clustering and fuzzy logic [144]. [36] The integration of SDN and machine learning increases the complexity of the network management, and the machine learning models for intrusion detection can be resource-intensive, posing challenges for deployment on low-power IoT devices. In [125] the hybrid trust-based system can introduce significant computational overhead. The complexity was significantly introduced in [140] by the proposed hybrid intrusion detection system (HIDS), which combines a decision tree classifier and a one-class Support Vector Machine classifier. In [106] the SMTrust may not be suitable for highly resource-constrained devices due to the computational overhead of trust calculations.

• Dynamic network conditions: some studies assume relatively stable network conditions, which might not be the case in highly dynamic mobile IoT environments [25] [54] [75] [138]. In [106] effectiveness of the SMTrust in highly dynamic environments with frequent topology changes needs further validation.

• Real-world testing: in some studies experiments were conducted in a simulation environment, which might not accurately reflect the complexity and unpredictability of actual IoT deployments [25] [26] [54] [58] [60] [75] [125] [138]-[140] [142] [144]. The experiments in [26] were conducted in a controlled environment, which may need to fully replicate the challenges and dynamics of real-world IoT deployment. In [36] the algorithm's performance has been validated in simulations, but real-world testing in diverse IoT environments is necessary to confirm its effectiveness.

• Energy consumption analysis: some studies evaluate the effectiveness of the proposed methods, but do not deeply analyze the impact on energy usage, which is vital for IoT devices that run on batteries [58] [60] [75] [125] [138] [139] [140] [142] [144]. In [25] the study evaluates performance metrics like end-to-end

latency and packet delivery ratio, but it does not analyze the energy usage impact. The studies in [26] [54] focus on detection accuracy and network performance, without extensive energy consumption investigation.

3. Future Research Directions and Technology

Several researchers adopted Artificial Intelligence (AI) or Blockchain (BC) technology in their proposed countermeasures for IoT routing attacks. AI is a vast field that covers Neural Networks (NNs), Deep Learning (DL), and Machine Learning (ML). ML is an AI method that helps systems learn from various datasets. DL uses a broad class of models called NNs. The area in which NNs are used is in DL. BC is a decentralized ledger which is composed of continuously expanding lists of entries (blocks) that are safely connected to one another by cryptographic hashes. Systematic reviews and critical studies of DL, ML, and their combination techniques for discovering RPL-based network attacks have been published in the literature [8]. A taxonomy for IIoT and IoT security along with BC-based potential solutions was provided [7]. **Table 6** provides a list of recent research work based on these technologies, which can be considered by interested researchers in the field.

Table 6. Summary of IoT routing's research based on innovative technologies.

Technology	Proposed Approach/Model	Addressed attacks	Ref.
Machine Learning (ML)	ML-based methods	DIS flooding	[21]
	ML light gradient boosting machine (ML-LGBM) model	Version number	[23]
	SDN and ML-based SRAIOT algorithm	DoS	[36]
	ML methods	Wormhole	[59]
	Support vector regressive trust-based security algorithm (TSVR)	Blackhole	[66]
	ML approaches	Sybil	[82]
	ML-based model	DoS, Blackhole, On-off	[103]
	Multiclass classification-based ML GBM (MC-MLGBM)	Rank, Wormhole	[123]
	ML approach	Rank, Version number, Blackhole, Sybil	[128]
	ML-based intrusion detection system	Decreased rank, Sinkhole, Blackhole, Selective forward., Hello flood., Version number	[129]
	ML approaches	Sinkhole, Sybil, Blackhole, Selective forward., DIO suppressing, DIS flood.	[133]
	ML-based intrusion detection system	Decreased rank, Blackhole, Sinkhole, Selective forward.	[137]
	ML-approaches	Hello flooding, Clone id, Selective forwarding, Blackhole, Sybil, Sinkhole	[143]

Continued

Deep Learning (DL)	A rider optimization approach based on bypass-linked attacker update (BAU-ROA)	Hello flooding	[16]
	DL approach	DoS	[35]
	Early-stage detection based on DL (DL-ESD)	Hello flooding, Decreased rank, Version number	[121]
	Hybrid DL-based Intrusion Detection System	DIS flooding, Increased rank, Decreased rank, Wormhole	[139]
	Trust-based attack detecting prototype	Different attacks	[145]
	ML-Based Data-Aggregation and Routing-Protocol (MLBDARP)	Different attacks	[146]
Neural Network (NN)	Artificial NN (ANN) Model	Decreased rank	[74]
	Dense NN (DNN) approach	Clone ID	[84]
Blockchain (BC)	BC-based solutions	IoT and IIoT security	[7]
	BC-based framework	Version number, Rank attacks	[109]
	Secure cluster-based routing protocol	IoT-based WSNs for smart agriculture	[147]
ML, DL	Review of ML and DL approaches	RPL-based IoT attacks	[8]
Q-Learning (QL)	QSec-RPL technique	Version number	[26]
Dynamic Bayesian Network (DBN)	Security authentication based on DBN combined with a trusted protocol	DoS	[30]
Artificial Intelligence (AI)	AI-based detection technique	Selective forwarding	[39]
TOPSIS and Hash-based Cryptography	TOPSIS decision-making and hash-based technique	Wormhole	[58]
Deep Reinforcement Learning (DRL)	QoS-aware secured routing protocol based on DRL (DQSP)	Blackhole, DoS	[102]
AI, ML	AI-enabled ML approach (AIEMLA)	Hello flooding, Decreased rank, Version number	[110]
Stochastic and Game Models	Game models-based anomaly intrusion detection system (GAIDS)	Rank, DIS flooding	[111]
Deep Q-learning (DQL)	DQNSec routing approach	Sinkhole, Hello flood, DDoS	[124]
Fuzzy Logic (FL)	Swan Intelligent based Clustering Technique (SICT)	Different attacks	[144]

3.1. Innovative Technologies

It appears that protecting IoT routing from attacks with innovative technologies like deep learning, artificial intelligence (AI), deep Q-learning, neural networks, machine learning, fuzzy logic, and blockchain will be possible in the future [148] [149]. These are a few important prospects:

- Artificial Intelligence and Machine Learning: As these technologies advance, more advanced anomaly detection and predictive analytics will be possible. IoT networks can become more resilient with AI's assistance in real-time threat detection and response.

• Deep Learning and neural networks will improve the capacity to spot intricate patterns and irregularities in IoT traffic. Convolutional and recurrent neural network techniques, for example, will be essential to creating intrusion detection systems with higher levels of accuracy.

• Deep Q-Learning: this reinforcement learning method can dynamically optimize routing choices, enhancing IoT security and efficiency.

• Fuzzy Logic: by addressing the ambiguity and imprecision in Internet of Things environments, fuzzy logic systems offer adaptable security measures. They can make decisions based on erratic inputs, which is crucial for IoT networks that are dynamic and complex.

• Blockchain: by offering decentralized and impenetrable ledgers, blockchain technology will be crucial to the routing security for Internet of Things networks. By doing this, the risk of attacks is decreased because data integrity and secure device communication are guaranteed.

When combined, these technologies will provide a strong and flexible security framework for Internet of Things routing that can counteract a variety of cyber-threats.

3.2. Recommendations for Future Research

By considering the above-mentioned limitations and innovative technologies the future research can effectively contribute to IoT routing security solutions. In particular, the following points can be addressed by future studies:

• Scalability testing: future studies should concentrate on testing the scalability of proposed protocols and algorithms in large-scale IoT networks.

• Resource efficiency: developing lightweight security solutions that can be deployed on resource-constrained IoT devices without compromising performance.

• Real-world validation: conducting real-world experiments to validate the effectiveness of proposed solutions in diverse IoT environments.

• Interoperability: addressing interoperability challenges to ensure seamless integration of different security frameworks and standards.

• Dynamic adaptation: creating adaptive security mechanisms that can respond to the continuously changing IoT networks and evolving threat landscapes.

4. Conclusion

As an outcome of the broad dispersion of modern Internet of Things (IoT) application domains, there are numerous security risks and attacks that might occur. Many researchers have worked hard to solve the routing protocol's security flaws in this area, particularly for IoT networks built on RPL. Despite multiple studies on the security of IoT routing protocols, routing attacks remain a top priority of ongoing research in IoT contexts. This paper describes and categorizes numerous routing attacks and their detrimental impact on IoT-based networks. Then, it carries out a thorough systematic review of existing IoT routing attacks and suggested countermeasure techniques. Specifically, it gives a summary of recently published

work on routing attacks with a primary focus on countermeasures, highlighting major security contributions, and drawing conclusions. Also, it discusses common shortcomings and limitations of the most recent studies. Finally, the study highlights innovative technological features and recommendations for future work. Thus, it offers a strong basis for researchers in the IoT routing security domain.

Acknowledgements

Support for this research work has been provided by the Deanship of Scientific Research at Prince Sattam bin Abdulaziz University.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Mrabet, H., Belguith, S., Alhomoud, A. and Jemai, A. (2020) A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*, **20**, Article 3625. https://doi.org/10.3390/s20133625

[2] Tournier, J., Lesueur, F., Mouël, F.L., Guyon, L. and Ben-Hassine, H. (2021) A Survey of IoT Protocols and Their Security Issues through the Lens of a Generic IoT Stack. *Internet of Things*, **16**, Article 100264. https://doi.org/10.1016/j.iot.2020.100264

[3] Sahay, R., Geethakumari, G. and Mitra, B. (2021) A Holistic Framework for Prediction of Routing Attacks in IoT-LLNs. *The Journal of Supercomputing*, **78**, 1409-1433. https://doi.org/10.1007/s11227-021-03922-1

[4] Boudouaia, M.A., Ali-Pacha, A., Abouaissa, A. and Lorenz, P. (2020) Security against Rank Attack in RPL Protocol. *IEEE Network*, **34**, 133-139. https://doi.org/10.1109/mnet.011.1900651

[5] Verma, A. and Ranga, V. (2020) Security of RPL Based 6lowpan Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, **20**, 5666-5690. https://doi.org/10.1109/jsen.2020.2973677

[6] Vaghela, R. and Upadhyay, D. (2020) A Survey on Routing Attacks in Internet of Things (IOT). *International Research Journal of Engineering and Technology*, **7**, 36-42.

[7] Sengupta, J., Ruj, S. and Das Bit, S. (2020) A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications*, **149**, Article 102481. https://doi.org/10.1016/j.jnca.2019.102481

[8] Al-Amiedy, T.A., Anbar, M., Belaton, B., Kabla, A.H.H., Hasbullah, I.H. and Alashhab, Z.R. (2022) A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. *Sensors*, **22**, Article 3400. https://doi.org/10.3390/s22093400

[9] Avila, K., Jabba, D. and Gomez, J. (2020) Security Aspects for RPL-Based Protocols: A Systematic Review in IoT. *Applied Sciences*, **10**, Article 6472. https://doi.org/10.3390/app10186472

[10] Bang, A.O., Rao, U.P., Kaliyar, P. and Conti, M. (2022) Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. *ACM Computing*

Surveys, **55**, 1-36. https://doi.org/10.1145/3494524

[11] Stephen, A. and Arockiam, L. (2021) Attacks against RPL in IoT: A Survey. *Annals of R.S.C.B.*, **25**, 9767-9786.

[12] Challa, R. and Rao, K.S. (2022) Resource Based Attacks Security Using RPL Protocol in Internet of Things. *Ingénierie des systèmes d information*, **27**, 165-170. https://doi.org/10.18280/isi.270120

[13] Akhtar, M.S. and Feng, T. (2022) A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms over IOT Layers. *ICST Transactions on Security and Safety*, **8**, e5. https://doi.org/10.4108/eetss.v8i30.590

[14] Wang, X., Ma, X., Peng, J., Li, J., Xue, L., Hu, W., *et al.* (2021) On Modeling Link Flooding Attacks and Defenses. *IEEE Access*, **9**, 159198-159217. https://doi.org/10.1109/access.2021.3131503

[15] Cakir, S., Toklu, S. and Yalcin, N. (2020) RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning. *IEEE Access*, **8**, 183678-183689. https://doi.org/10.1109/access.2020.3029191

[16] Aditya Sai Srinivas, T. and Manivannan, S.S. (2020) Prevention of Hello Flood Attack in IoT Using Combination of Deep Learning with Improved Rider Optimization Algorithm. *Computer Communications*, **163**, 162-175. https://doi.org/10.1016/j.comcom.2020.03.031

[17] Hkiri, A., Alqurashi, S., Ben Bahri, O., Karmani, M., Faraj, H. and Machhout, M. (2024) Performance Evaluation of Mobile RPL-Based IoT Networks under Hello Flood Attack. *Electronics*, **13**, Article 2226. https://doi.org/10.3390/electronics13112226

[18] Abhinaya, E.V. and Sudhakar, B. (2021) A Secure Routing Protocol for Low Power and Lossy Networks Based 6LoWPAN Networks to Mitigate DIS Flooding Attacks. *Journal of Ambient Intelligence and Humanized Computing*, **12**, 1-12. https://doi.org/10.1007/s12652-020-02804-3

[19] Medjek, F., Tandjaoui, D., Djedjig, N. and Romdhani, I. (2021) Multicast DIS Attack Mitigation in RPL-Based IoT-LLNs. *Journal of Information Security and Applications*, **61**, Article 102939. https://doi.org/10.1016/j.jisa.2021.102939

[20] Verma, A. and Ranga, V. (2019) Mitigation of DIS Flooding Attacks in RPL-Based 6LoWPAN Networks. *Transactions on Emerging Telecommunications Technologies*, **31**, e3802. https://doi.org/10.1002/ett.3802

[21] Çakir, S. and Yalçin, N. (2021) Detection of DIS Flooding Attacks in IoT Networks Using Machine Learning Methods. *European Journal of Science and Technology*, **28**, 1317-1320. https://doi.org/10.31590/ejosat.1014917

[22] Rajasekar, V.R. and Rajkumar, S. (2022) A Study on Impact of DIS Flooding Attack on RPL-Based 6LoWPAN Network. *Microprocessors and Microsystems*, **94**, Article 104675. https://doi.org/10.1016/j.micpro.2022.104675

[23] Osman, M., He, J., Mokbal, F.M.M., Zhu, N. and Qureshi, S. (2021) ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks. *IEEE Access*, **9**, 83654-83665. https://doi.org/10.1109/access.2021.3087175

[24] Sahay, R., Geethakumari, G., Mitra, B. and Sahoo, I. (2019) Efficient Framework for Detection of Version Number Attack in Internet of Things. In: Abraham, A., Cherukuri, A.K., Melin, P. and Gandhi, N., Eds., *Intelligent Systems Design and Applications*, Springer, 480-492. https://doi.org/10.1007/978-3-030-16660-1_47

[25] Sharma, G., Grover, J. and Verma, A. (2023) Performance Evaluation of Mobile RPL-Based IoT Networks under Version Number Attack. *Computer Communications*, **197**, 12-22. https://doi.org/10.1016/j.comcom.2022.10.014

[26] Sharma, G., Grover, J. and Verma, A. (2023) QSec-RPL: Detection of Version Number Attacks in RPL Based Mobile IoT Using Q-learning. *Ad Hoc Networks*, **142**, Article 103118. https://doi.org/10.1016/j.adhoc.2023.103118

[27] Alfriehat, N.A., Anbar, M., Karuppayah, S., Rihan, S.D.A., Alabsi, B.A. and Momani, A.M. (2024) Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy. *IEEE Access*, **12**, 31136-31158. https://doi.org/10.1109/access.2024.3368633

[28] Rahamathullah, U. and Karthikeyan, E. (2021) A Lightweight Trust-Based System to Ensure Security on the Internet of Battlefield Things (IoBT) Environment. *International Journal of System Assurance Engineering and Management*, **12**, 1-13. https://doi.org/10.1007/s13198-021-01250-4

[29] Kannan, S., Reddy, G.F.H. and Rajesh, M. (2020) Novel Approach Using Optimized Trustable Route Node Convention Technique with Robust Security for Mobile Ad Hoc Networks in IoT. *Oxidation Communications*, **43**, 39-53.

[30] Zhang, Q. and Xu, D. (2018) Security Authentication Technology Based on Dynamic Bayesian Network in Internet of Things. *Journal of Ambient Intelligence and Humanized Computing*, **11**, 573-580. https://doi.org/10.1007/s12652-018-0949-2

[31] Verma, A. and Ranga, V. (2020) The Impact of Copycat Attack on RPL Based 6LoWPAN Networks in Internet of Things. *Computing*, **103**, 1479-1500. https://doi.org/10.1007/s00607-020-00862-1

[32] Alamiedy, T.A., Anbar, M.F.R., Belaton, B., Kabla, A.H. and Khudayer, B.H. (2021) Ensemble Feature Selection Approach for Detecting Denial of Service Attacks in RPL Networks. In: Abdullah, N., Manickam, S. and Anbar, M., Eds., *Advances in Cyber Security*, Springer, 340-360. https://doi.org/10.1007/978-981-16-8059-5_21

[33] Al-Sadoon, M. and Jedidi, A. (2022) A Secure Trust-Based Protocol for Hierarchical Routing in Wireless Sensor Network. *International Journal of Electrical and Computer Engineering*, **12**, 3838-3849. https://doi.org/10.11591/ijece.v12i4.pp3838-3849

[34] Karthikeyan, H. and Usha, G. (2022) Real-Time DDoS Flooding Attack Detection in Intelligent Transportation Systems. *Computers and Electrical Engineering*, **101**, Article 107995. https://doi.org/10.1016/j.compeleceng.2022.107995

[35] Hasan, A.H., Anbar, M. and Alamiedy, T.A. (2022) Deep Learning Approach for Detecting Router Advertisement Flooding-Based DDoS Attacks. *Journal of Ambient Intelligence and Humanized Computing*, **14**, 7281-7295. https://doi.org/10.1007/s12652-022-04437-0

[36] Rui, K., Pan, H. and Shu, S. (2023) Secure Routing in the Internet of Things (IoT) with Intrusion Detection Capability Based on Software-Defined Networking (SDN) and Machine Learning Techniques. *Scientific Reports*, **13**, Article No. 18003. https://doi.org/10.1038/s41598-023-44764-6

[37] Fotohi, R. and Pakdel, H. (2021) A Lightweight and Scalable Physical Layer Attack Detection Mechanism for the Internet of Things (IoT) Using Hybrid Security Schema. *Wireless Personal Communications*, **119**, 3089-3106. https://doi.org/10.1007/s11277-021-08388-1

[38] Chakraborty, M., Spanò, A. and Cortesi, A. (2021) Geographic Location Based Secure, Dynamic and Opportunistic RPL for Distributed Networks. *Ad Hoc Networks*, **123**, Article 102689. https://doi.org/10.1016/j.adhoc.2021.102689

[39] Neerugatti, V. and Rama Mohan Reddy, A. (2020) Artificial Intelligence-Based Technique for Detection of Selective Forwarding Attack in RPL-Based Internet of Things Networks. In: Krishna, P.V. and Obaidat, M.S., Eds., *Emerging Research in Data Engineering Systems and Computer Communications*, Springer, 67-77. https://doi.org/10.1007/978-981-15-0135-7_7

[40] Jiang, J. and Liu, Y. (2022) Secure IoT Routing—Selective Forwarding Attacks and Trust-Based Defences in RPL Network.

[41] Adarbah, H.Y. and Ahmad, S. (2022) Impact of Selective Forwarding Attacks on the Performance of RPL Routing Protocol in the Internet of Things. *International Journal of Research Publication and Reviews*, **3**, 1479-1487.

[42] Prathapchandran, K. and Janani, T. (2021) A Trust Aware Security Mechanism to Detect Sinkhole Attack in RPL-Based IoT Environment Using Random Forest—RFTRUST. *Computer Networks*, **198**, Article 108413. https://doi.org/10.1016/j.comnet.2021.108413

[43] Zaminkar, M. and Fotohi, R. (2020) Sos-rpl: Securing Internet of Things against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism. *Wireless Personal Communications*, **114**, 1287-1312. https://doi.org/10.1007/s11277-020-07421-z

[44] Tabari, M.Y. and Mataji, Z. (2021) Detecting Sinkhole Attack in RPL-Based Internet of Things Routing Protocol. *Journal of Artificial Intelligence and Data Mining*, **9**, 73-85.

[45] Omar, A.A.A., Soudan, B. and Altaweel, A. (2023) A Comprehensive Survey on Detection of Sinkhole Attack in Routing over Low Power and Lossy Network for Internet of Things. *Internet of Things*, **22**, Article 100750. https://doi.org/10.1016/j.iot.2023.100750

[46] Mondal, K., Yadav, S.S., Pal, V., Singh, A.P., Yogita, Y. and Singh, M. (2022) Detecting Sinkhole Attacks in IoT-Based Wireless Sensor Networks Using Distance from Base Station. *International Journal of Information System Modeling and Design*, **13**, 1-18. https://doi.org/10.4018/ijismd.297628

[47] Bilal, A., Hasany, S.M.N. and Pitafi, A.H. (2022) Effective Modelling of Sinkhole Detection Algorithm for Edge-Based Internet of Things (IoT) Sensing Devices. *IET Communications*, **16**, 845-855. https://doi.org/10.1049/cmu2.12385

[48] An, G.H. and Cho, T.H. (2022) Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT. *International Journal of Computer Networks and Applications*, **9**, 169-178. https://doi.org/10.22247/ijcna/2022/212333

[49] Parkavi, T. and Arockiam, L. (2021) A Survey on Sinkhole Attack in RPL. *Annals of the Romanian Society for Cell Biology*, **25**, 511-515. http://annalsofrscb.ro/index.php/journal/article/view/4322

[50] Pundir, S., Wazid, M., Singh, D.P., Das, A.K., J. P. C. Rodrigues, J.J.P.C. and Park, Y. (2020) Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment. *Sensors*, **20**, Article 1300. https://doi.org/10.3390/s20051300

[51] Patel, B. and Shah, P. (2021) Direct Neighbour Sink Reputed Trust Based Intrusion Detection System to Mitigate Sinkhole Attack in RPL for IoT Networks. *Journal of Engineering Science and Technology Review*, **14**, 38-35. https://doi.org/10.25103/jestr.141.03

[52] Patel, B.H. and Shah, P. (2020) RPL Routing Protocol Performance under Sinkhole and Selective Forwarding Attack: Experimental and Simulated Evaluation. *Telecommunication Computing Electronics and Control*, **18**, 1849-1856.

https://doi.org/10.12928/telkomnika.v18i4.15768

[53] Srinivas, T.A.S. and Manivannan, S.S. (2021) Black Hole and Selective Forwarding Attack Detection and Prevention in IoT in Health Care Sector: Hybrid Meta-Heuristic-Based Shortest Path Routing. *Journal of Ambient Intelligence and Smart Environments*, **13**, 133-156. https://doi.org/10.3233/ais-210591

[54] Alansari, Z., Anuar, N.B., Kamsin, A. and Belgaum, M.R. (2023) RPLAD3: Anomaly Detection of Blackhole, Grayhole, and Selective Forwarding Attacks in Wireless Sensor Network-Based Internet of Things. *Peer J Computer Science*, **9**, e1309. https://doi.org/10.7717/peerj-cs.1309

[55] Bhosale, S.A. and Sonavane, S.S. (2021) Wormhole Attack Detection System for IoT Network: A Hybrid Approach. *Wireless Personal Communications*, **124**, 1081-1108. https://doi.org/10.1007/s11277-021-09395-y

[56] Parvathy, K. (2021) Wormhole Attacks in Wireless Sensor Networks (WSN) & Internet of Things (IoT): A Review. *International Journal of Recent Technology and Engineering*, **10**, 199-203. https://doi.org/10.35940/ijrte.a5873.0510121

[57] Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. and A. AlZain, M. (2021) Energy Optimized Security against Wormhole Attack in IoT-Based Wireless Sensor Networks. *Computers, Materials & Continua*, **68**, 1967-1981. https://doi.org/10.32604/cmc.2021.015259

[58] Sahraneshin, T., Malekhosseini, R., Rad, F. and Yaghoubyan, S.H. (2022) Securing Communications between Things against Wormhole Attacks Using TOPSIS Decision-Making and Hash-Based Cryptography Techniques in the IoT Ecosystem. *Wireless Networks*, **29**, 969-983. https://doi.org/10.1007/s11276-022-03169-5

[59] Priyadarshini, R., Alagirisamy, M., Rajendran, N. and Varunkumar, K.A. (2022) Invalidation of Tunnelling Attacks in Ubiquitous IoT & Wireless Sensor Enviroment Using ML Methods. *Optik*, **271**, Article 170163. https://doi.org/10.1016/j.ijleo.2022.170163

[60] Javed, S., Sajid, A., Kiren, T., Khan, I.U., Dewi, C., Cauteruccio, F., *et al.* (2023) A Subjective Logical Framework-Based Trust Model for Wormhole Attack Detection and Mitigation in Low-Power and Lossy (RPL) IoT-Networks. *Information*, **14**, Article 478. https://doi.org/10.3390/info14090478

[61] VenkataRao, S. and Ananth, V. (2021) A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN. *International Journal of Intelligent Engineering and Systems*, **14**, 498-506

[62] Sharma, D.K., Dhurandher, S.K., Kumaram, S., Gupta, K.D. and Sharma, P.K. (2022) Mitigation of Black Hole Attacks in 6LoWPAN RPL-Based Wireless Sensor Network for Cyber Physical Systems. *Computer Communications*, **189**, 182-192.

[63] Kandhoul, N. and Dhurandher, S.K. (2021) An Efficient and Secure Data Forwarding Mechanism for Opportunistic IoT. *Wireless Personal Communications*, **118**, 217-237. https://doi.org/10.1007/s11277-020-08010-w

[64] Malik, A., Khan, M.Z., Faisal, M., Khan, F. and Seo, J. (2022) An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in Vanets. *Sensors*, **22**, Article 1897. https://doi.org/10.3390/s22051897

[65] Srinivasan, V. (2021) Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on Manet. *Ingénierie des systèmes d information*, **26**, 549-557. https://doi.org/10.18280/isi.260605

[66] Rutravigneshwaran, P., Anitha, G. and Prathapchandran, K. (2022) Trust-Based Support Vector Regressive (TSVR) Security Mechanism to Identify Malicious Nodes in the Internet of Battlefield Things (IoBT). *International Journal of System Assurance*

Engineering and Management, **15**, 287-299.
https://doi.org/10.1007/s13198-022-01719-w

[67] ul Hassan, T., Asim, M., Baker, T., Hassan, J. and Tariq, N. (2021) *CTrust-RPL*: A Control Layer-Based Trust Mechanism for Supporting Secure Routing in Routing Protocol for Low Power and Lossy Networks-Based Internet of Things Applications. *Transactions on Emerging Telecommunications Technologies*, **32**, e4224.
https://doi.org/10.1002/ett.4224

[68] Kale, S. and Bhosale, S. (2021) Detection of Blackhole Attack in IoT. *IT in Industry*, **9**, 1-8.

[69] Srinivas, T.A.S. and Manivannan, S.S.M. (2020) Preventing Collaborative Black Hole Attack in IoT Construction Using a CBHA–AODV Routing Protocol. *International Journal of Grid and High Performance Computing*, **12**, 25-46.
https://doi.org/10.4018/ijghpc.2020040102

[70] Luangoudom, S., Tran, D., Nguyen, T., Tran, H.A., Nguyen, G. and Ha, Q.T. (2020) Svblock: Mitigating Black Hole Attack in Low-Power and Lossy Networks. *International Journal of Sensor Networks*, **32**, 77-86.
https://doi.org/10.1504/ijsnet.2020.104923

[71] Hasan, A., Khan, M.A., Shabir, B., Munir, A., Malik, A.W., Anwar, Z., *et al.* (2022) Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things. *Applied Sciences*, **12**, Article 11442. https://doi.org/10.3390/app122211442

[72] Safdar Malik, T., Siddiqui, M.N., Mateen, M., Malik, K.R., Sun, S. and Wen, J. (2022) Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring. *Security and Communication Networks*, **2022**, 1-18.
https://doi.org/10.1155/2022/4943218

[73] Kiran, V., Rani, S. and Singh, P. (2019) Towards a Light Weight Routing Security in IoT Using Non-Cooperative Game Models and Dempster–Shaffer Theory. *Wireless Personal Communications*, **110**, 1729-1749.
https://doi.org/10.1007/s11277-019-06809-w

[74] Osman, M., He, J., Mokbal, F.M. and Zhu, N. (2021) Artificial Neural Network Model for Decreased Rank Attack Detection in RPL Based on IoT Networks. *International Journal of Network Security*, **23**, 497-504.

[75] Rouissat, M., Belkehir, M., Mokaddem, A., Bouziani, M. and Alsukayti, I.S. (2024) Exploring and Mitigating Hybrid Rank Attack in RPL-Based IoT Networks. *Journal of Electrical Engineering*, **75**, 204-213. https://doi.org/10.2478/jee-2024-0025

[76] Bang, A.O. and Rao, U.P. (2021) A Novel Decentralized Security Architecture against Sybil Attack in RPL-Based IoT Networks: A Focus on Smart Home Use Case. *The Journal of Supercomputing*, **77**, 13703-13738.
https://doi.org/10.1007/s11227-021-03816-2

[77] Murali, S. and Jamalipour, A. (2020) A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things. *IEEE Internet of Things Journal*, **7**, 379-388. https://doi.org/10.1109/jiot.2019.2948149

[78] Pu, C. (2020) Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses. *IEEE Internet of Things Journal*, **7**, 4937-4949.
https://doi.org/10.1109/jiot.2020.2971463

[79] Hassan, J., Sohail, A., Awad, A.I. and Zaka, M.A. (2024) LETM-IoT: A Lightweight and Efficient Trust Mechanism for Sybil Attacks in Internet of Things Networks. *Ad Hoc Networks*, **163**, Article 103576. https://doi.org/10.1016/j.adhoc.2024.103576

[80] Arshad, A., Mohd Hanapi, Z., Subramaniam, S. and Latip, R. (2021) A Survey of Sybil

Attack Countermeasures in IoT-Based Wireless Sensor Networks. *Peer J Computer Science*, **7**, e673. https://doi.org/10.7717/peerj-cs.673

[81] Thuluva, A.S.S., Somanathan, M.S., Somula, R., Sennan, S. and Burgos, D. (2021) Secure and Efficient Transmission of Data Based on Caesar Cipher Algorithm for Sybil Attack in IoT. *EURASIP Journal on Advances in Signal Processing*, **2021**, Article No. 38. https://doi.org/10.1186/s13634-021-00748-0

[82] Mehbodniya, A., Webber, J.L., Shabaz, M., Mohafez, H. and Yadav, K. (2021) RETRACTED ARTICLE: Machine Learning Technique to Detect Sybil Attack on IoT Based Sensor Network. *IETE Journal of Research*, **69**, 1-9. https://doi.org/10.1080/03772063.2021.2000509

[83] Arshad, D., Asim, M., Tariq, N., Baker, T., Tawfik, H. and Al-Jumeily OBE, D. (2022) THC-RPL: A Lightweight Trust-Enabled Routing in RPL-Based IoT Networks against Sybil Attack. *PLOS ONE*, **17**, e0271277. https://doi.org/10.1371/journal.pone.0271277

[84] Morales-Molina, C.D., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L.K., Perez-Meana, H., Olivares-Mercado, J., *et al.* (2021) A Dense Neural Network Approach for Detecting Clone ID Attacks on the RPL Protocol of the IoT. *Sensors*, **21**, Article 3173. https://doi.org/10.3390/s21093173

[85] Vaishnavi, S. and Sethukarasi, T. (2022) Detection and Avoidance of Clone Attack in IoT Based Smart Health Application. *Intelligent Automation & Soft Computing*, **31**, 1919-1937. https://doi.org/10.32604/iasc.2022.021006

[86] Kore, A. and Patil, S. (2022) Cross Layered Cryptography Based Secure Routing for IoT-Enabled Smart Healthcare System. *Wireless Networks*, **28**, 287-301. https://doi.org/10.1007/s11276-021-02850-5

[87] G, I.L. and Kavitha, V. (2021) Privacy Preserving Using Multi-Hop Dynamic Clustering Routing Protocol and Elliptic Curve Cryptosystem for WSN in IoT Environment. *Peer-to-Peer Networking and Applications*, **14**, 821-836. https://doi.org/10.1007/s12083-020-01038-6

[88] Meena, U. and Sharma, P. (2022) Secret Dynamic Key Authentication and Decision Trust Secure Routing Framework for Internet of Things Based WSN. *Wireless Personal Communications*, **125**, 1753-1781. https://doi.org/10.1007/s11277-022-09632-y

[89] Conti, M., Kaliyar, P., Rabbani, M.M. and Ranise, S. (2020) Attestation-Enabled Secure and Scalable Routing Protocol for IoT Networks. *Ad Hoc Networks*, **98**, Article 102054. https://doi.org/10.1016/j.adhoc.2019.102054

[90] Alotaibi, M. (2021) Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN. *IEEE Access*, **9**, 159187-159197. https://doi.org/10.1109/access.2021.3130005

[91] Simoglou, G., Violettas, G., Petridou, S. and Mamatas, L. (2021) Intrusion Detection Systems for RPL Security: A Comparative Analysis. *Computers & Security*, **104**, Article 102219. https://doi.org/10.1016/j.cose.2021.102219

[92] Pasikhani, A.M., Clark, J.A., Gope, P. and Alshahrani, A. (2021) Intrusion Detection Systems in RPL-Based 6lowpan: A Systematic Literature Review. *IEEE Sensors Journal*, **21**, 12940-12968. https://doi.org/10.1109/jsen.2021.3068240

[93] Sahay, R., Geethakumari, G. and Mitra, B. (2022) Mitigating the Worst Parent Attack in RPL Based Internet of Things. *Cluster Computing*, **25**, 1303-1320. https://doi.org/10.1007/s10586-021-03528-5

[94] Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A. and Buchanan, W.J. (2020) Mitigation Mechanisms against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL). *IEEE Access*, **8**, 43665-43675. https://doi.org/10.1109/access.2020.2977476

[95] Anajemba, J.H., Tang, Y., Iwendi, C., Ohwoekevwo, A., Srivastava, G. and Jo, O. (2020) Realizing Efficient Security and Privacy in IoT Networks. *Sensors*, **20**, Article 2609. https://doi.org/10.3390/s20092609

[96] Bang, A.O. and Rao, U.P. (2022) EMBOF-RPL: Improved RPL for Early Detection and Isolation of Rank Attack in RPL-Based Internet of Things. *Peer-to-Peer Networking and Applications*, **15**, 642-665. https://doi.org/10.1007/s12083-021-01275-3

[97] Seyfollahi, A., Moodi, M. and Ghaffari, A. (2022) MFO-RPL: A Secure RPL-Based Routing Protocol Utilizing Moth-Flame Optimizer for the IoT Applications. *Computer Standards & Interfaces*, **82**, Article 103622. https://doi.org/10.1016/j.csi.2022.103622

[98] Nandhini, P.S., Kuppuswami, S., Malliga, S. and DeviPriya, R. (2022) Enhanced Rank Attack Detection Algorithm (E-RAD) for Securing RPL-Based IoT Networks by Early Detection and Isolation of Rank Attackers. *The Journal of Supercomputing*, **79**, 6825-6848. https://doi.org/10.1007/s11227-022-04921-6

[99] Nandhini, P.S., Kuppuswami, S., Malliga, S. and DeviPriya, R. (2022) A Lightweight Energy-Efficient Algorithm for Mitigation and Isolation of Internal Rank Attackers in RPL Based Internet of Things. *Computer Networks*, **218**, Article 109391. https://doi.org/10.1016/j.comnet.2022.109391

[100] Deebak, B.D. and Al-Turjman, F. (2020) A Hybrid Secure Routing and Monitoring Mechanism in IoT-Based Wireless Sensor Networks. *Ad Hoc Networks*, **97**, Article 102022. https://doi.org/10.1016/j.adhoc.2019.102022

[101] Gali, S. and Nidumolu, V. (2021) An Intelligent Trust Sensing Scheme with Metaheuristic Based Secure Routing Protocol for Internet of Things. *Cluster Computing*, **25**, 1779-1789. https://doi.org/10.1007/s10586-021-03473-3

[102] Guo, X., Lin, H., Li, Z. and Peng, M. (2020) Deep-Reinforcement-Learning-Based QoS-Aware Secure Routing for SDN-IoT. *IEEE Internet of Things Journal*, **7**, 6242-6251. https://doi.org/10.1109/jiot.2019.2960033

[103] Farea, A.H. and Küçük, K. (2022) Detections of IoT Attacks via Machine Learning-Based Approaches with Cooja. *EAI Endorsed Transactions on Internet of Things*, **7**, 1-12. https://doi.org/10.4108/eetiot.v7i28.324

[104] Verma, A. and Ranga, V. (2020) Cosec-RPL: Detection of Copycat Attacks in RPL Based 6LoWPANs Using Outlier Analysis. *Telecommunication Systems*, **75**, 43-61. https://doi.org/10.1007/s11235-020-00674-w

[105] Stute, M., Agarwal, P., Kumar, A., Asadi, A. and Hollick, M. (2020) LIDOR: A Lightweight DoS-Resilient Communication Protocol for Safety-Critical IoT Systems. *IEEE Internet of Things Journal*, **7**, 6802-6816. https://doi.org/10.1109/jiot.2020.2985044

[106] Muzammal, S.M., Murugesan, R.K., Jhanjhi, N., Hossain, M.S. and Yassine, A. (2022) Trust and Mobility-Based Protocol for Secure Routing in Internet of Things. *Sensors*, **22**, Article 6215. https://doi.org/10.3390/s22166215

[107] Muzammal, S.M., Murugesan, R.K., Jhanjhi, N.Z., Humayun, M., Ibrahim, A.O. and Abdelmaboud, A. (2022) A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things. *Sensors*, **22**, Article 7052. https://doi.org/10.3390/s22187052

[108] Kaliyar, P., Jaballah, W.B., Conti, M. and Lal, C. (2020) LIDL: Localization with Early Detection of Sybil and Wormhole Attacks in IoT Networks. *Computers & Security*, **94**, Article 101849. https://doi.org/10.1016/j.cose.2020.101849

[109] Sahay, R., Geethakumari, G. and Mitra, B. (2020) A Novel Blockchain Based Framework to Secure IoT-LLNs against Routing Attacks. *Computing*, **102**, 2445-2470. https://doi.org/10.1007/s00607-020-00823-8

[110] Sharma, S. and Verma, V.K. (2021) AIEMLA: Artificial Intelligence Enabled Machine Learning Approach for Routing Attacks on Internet of Things. *The Journal of Supercomputing*, **77**, 13757-13787. https://doi.org/10.1007/s11227-021-03833-1

[111] Gothawal, D.B. and Nagaraj, S.V. (2019) Anomaly-Based Intrusion Detection System in RPL by Applying Stochastic and Evolutionary Game Models over IoT Environment. *Wireless Personal Communications*, **110**, 1323-1344. https://doi.org/10.1007/s11277-019-06789-x

[112] Kalyani, G. and Chaudhari, S. (2021) Cross Layer Security MAC Aware Routing Protocol for IoT Networks. *Wireless Personal Communications*, **123**, 935-957. https://doi.org/10.1007/s11277-021-09163-y

[113] A. Almusaylim, Z., Jhanjhi, N. and Alhumam, A. (2020) Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP. *Sensors*, **20**, Article 5997. https://doi.org/10.3390/s20215997

[114] Raoof, A., Matrawy, A. and Lung, C. (2020) Enhancing Routing Security in IoT: Performance Evaluation of RPL's Secure Mode under Attacks. *IEEE Internet of Things Journal*, **7**, 11536-11546. https://doi.org/10.1109/jiot.2020.3022276

[115] Bettoumi, B. and Bouallegue, R. (2021) LC-DEX: Lightweight and Efficient Compressed Authentication Based Elliptic Curve Cryptography in Multi-Hop 6LoWPAN Wireless Sensor Networks in Hip-Based Internet of Things. *Sensors*, **21**, Article 7348. https://doi.org/10.3390/s21217348

[116] Almusaylim, Z.A., Alhumam, A. and Jhanjhi, N.Z. (2020) Proposing a Secure RPL Based Internet of Things Routing Protocol: A Review. *Ad Hoc Networks*, **101**, Article 102096. https://doi.org/10.1016/j.adhoc.2020.102096

[117] Kalyani, G. and Chaudhari, S. (2021) Security Aware Routing: Rule Based Attack Detection on Optimal Shortest Route Selection. *Ad Hoc & Sensor Wireless Networks*, **49**, 223-245.

[118] Sharma, S. and Verma, V.K. (2020) Security Explorations for Routing Attacks in Low Power Networks on Internet of Things. *The Journal of Supercomputing*, **77**, 4778-4812. https://doi.org/10.1007/s11227-020-03471-z

[119] Djedjig, N., Tandjaoui, D., Medjek, F. and Romdhani, I. (2020) Trust-Aware and Cooperative Routing Protocol for IoT Security. *Journal of Information Security and Applications*, **52**, Article 102467. https://doi.org/10.1016/j.jisa.2020.102467

[120] Ilyas, M., Ullah, Z., Khan, F.A., Chaudary, M.H., Malik, M.S.A., Zaheer, Z., *et al.* (2020) Trust-Based Energy-Efficient Routing Protocol for Internet of Things-Based Sensor Networks. *International Journal of Distributed Sensor Networks*, **16**, Article 155014772096435. https://doi.org/10.1177/1550147720964358

[121] Albishari, M., Li, M., Zhang, R. and Almosharea, E. (2022) Deep Learning-Based Early Stage Detection (DL-ESD) for Routing Attacks in Internet of Things Networks. *The Journal of Supercomputing*, **79**, 2626-2653. https://doi.org/10.1007/s11227-022-04753-4

[122] Mujtaba, A., Amjad, S., Rafiq, A., Mubarik, A. and Younus, M.U. (2022) Enhancement of accuracy of the Rank Inconsistency Detection Algorithm. *Pakistan Journal*

of Engineering and Applied Sciences, **30**, 61-75.

[123] Zahra, F., Jhanjhi, N., Brohi, S.N., Khan, N.A., Masud, M. and AlZain, M.A. (2022) Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning. *Sensors*, **22**, Article 6765. https://doi.org/10.3390/s22186765

[124] Kandhoul, N. and Dhurandher, S.K. (2022) Deep Q Learning Based Secure Routing Approach for OppIoT Networks. *Internet of Things*, **20**, Article 100597. https://doi.org/10.1016/j.iot.2022.100597

[125] Remya, S., Pillai, M.J., Arjun, C., Ramasubbareddy, S. and Cho, Y. (2024) Enhancing Security in LLNs Using a Hybrid Trust-Based Intrusion Detection System for RPL. *IEEE Access*, **12**, 58836-58850. https://doi.org/10.1109/access.2024.3391918

[126] Qureshi, K.N., Rana, S.S., Ahmed, A. and Jeon, G. (2020) A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things. *Sustainable Cities and Society*, **61**, Article 102343. https://doi.org/10.1016/j.scs.2020.102343

[127] Ioulianou, P.P., Vassilakis, V.G. and Shahandashti, S.F. (2022) A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks. *Journal of Cybersecurity and Privacy*, **2**, 124-153. https://doi.org/10.3390/jcp2010009

[128] Foley, J., Moradpoor, N. and Ochenyi, H. (2020) Employing a Machine Learning Approach to Detect Combined Internet of Things Attacks against Two Objective Functions Using a Novel Dataset. *Security and Communication Networks*, **2020**, 1-17. https://doi.org/10.1155/2020/2804291

[129] Medjek, F., Tandjaoui, D., Djedjig, N. and Romdhani, I. (2021) Fault-Tolerant Ai-Driven Intrusion Detection System for the Internet of Things. *International Journal of Critical Infrastructure Protection*, **34**, Article 100436. https://doi.org/10.1016/j.ijcip.2021.100436

[130] Hashemi, S.Y. and Shams Aliee, F. (2020) Fuzzy, Dynamic and Trust Based Routing Protocol for IoT. *Journal of Network and Systems Management*, **28**, 1248-1278. https://doi.org/10.1007/s10922-020-09535-y

[131] Farooq, U., Asim, M., Tariq, N., Baker, T. and Awad, A.I. (2022) Multi-Mobile Agent Trust Framework for Mitigating Internal Attacks and Augmenting RPL Security. *Sensors*, **22**, Article 4539. https://doi.org/10.3390/s22124539

[132] Sahraoui, S. and Henni, N. (2021) SAMP-RPL: Secure and Adaptive Multipath RPL for Enhanced Security and Reliability in Heterogeneous IoT-Connected Low Power and Lossy Networks. *Journal of Ambient Intelligence and Humanized Computing*, **14**, 409-429. https://doi.org/10.1007/s12652-021-03303-9

[133] Bokka, R. and Sadasivam, D.T. (2021) Machine Learning Techniques to Detect Routing Attacks in RPL Based Internet of Things. *International Journal of Electrical Engineering and Technology*, **12**, 346-356.

[134] Sithik, M.M. and Kumar, B.M. (2022) Intelligent Agent Based Virtual Clustering and Multi-Context Aware Routing for Congestion Mitigation in Secure RPL-IoT Environment. *Ad Hoc Networks*, **137**, Article 102972. https://doi.org/10.1016/j.adhoc.2022.102972

[135] Garcia Ribera, E., Martinez Alvarez, B., Samuel, C., Ioulianou, P.P. and Vassilakis, V.G. (2022) An Intrusion Detection System for RPL-Based IoT Networks. *Electronics*, **11**, Article 4041. https://doi.org/10.3390/electronics11234041

[136] Belavagi, M.C. and Muniyal, B. (2020) Multiple Intrusion Detection in RPL Based Networks. *International Journal of Electrical and Computer Engineering*, **10**, 467-476. https://doi.org/10.11591/ijece.v10i1.pp467-476

[137] Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Santhosh Kumar, S. and Kannan, A. (2022) An Intelligent RPL Attack Detection Using Machine Learning-Based Intrusion Detection System for Internet of Things. *Procedia Computer Science*, **215**, 61-70. https://doi.org/10.1016/j.procs.2022.12.007

[138] Alsukayti, I.S. and Alreshoodi, M. (2023) RPL-Based IoT Networks under Simple and Complex Routing Security Attacks: An Experimental Study. *Applied Sciences*, **13**, Article 4878. https://doi.org/10.3390/app13084878

[139] Al Sawafi, Y., Touzene, A. and Hedjam, R. (2023) Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. *Journal of Sensor and Actuator Networks*, **12**, Article 21. https://doi.org/10.3390/jsan12020021

[140] Alazab, A., Khraisat, A., Singh, S., Bevinakoppa, S. and Mahdi, O.A. (2023) Routing Attacks Detection in 6LoWPAN-Based Internet of Things. *Electronics*, **12**, Article 1320. https://doi.org/10.3390/electronics12061320

[141] Hussain, M.Z. and Hanapi, Z.M. (2023) Efficient Secure Routing Mechanisms for the Low-Powered IoT Network: A Literature Review. *Electronics*, **12**, Article 482. https://doi.org/10.3390/electronics12030482

[142] Hosseinzadeh, M., Yoo, J., Ali, S., Lansky, J., Mildeova, S., Yousefpoor, M.S., *et al.* (2023) A Fuzzy Logic-Based Secure Hierarchical Routing Scheme Using Firefly Algorithm in Internet of Things for Healthcare. *Scientific Reports*, **13**, Article No. 11058. https://doi.org/10.1038/s41598-023-38203-9

[143] Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M. and Hashemi, S.H. (2023) A Review on the Security of IoT Networks: From Network Layer's Perspective. *IEEE Access*, **11**, 71073-71087. https://doi.org/10.1109/access.2023.3246180

[144] Shanmugapriya, R. and SVN, S.K. (2024) An Energy Efficient Swan Intelligent Based Clustering Technique (SICT) with Fuzzy Based Secure Routing Protocol in IoT. *Peer-to-Peer Networking and Applications*, **17**, 1830-1864. https://doi.org/10.1007/s12083-024-01670-6

[145] Ahmadi, K. and Javidan, R. (2024) A Novel RPL Defense Mechanism Based on Trust and Deep Learning for Internet of Things. *The Journal of Supercomputing*, **80**, 16979-17003. https://doi.org/10.1007/s11227-024-06118-5

[146] Chandnani, N. and Khairnar, C.N. (2023) A Reliable Protocol for Data Aggregation and Optimized Routing in IoT WSNs Based on Machine Learning. *Wireless Personal Communications*, **130**, 2589-2622. https://doi.org/10.1007/s11277-023-10393-5

[147] Rao, A.K., Nagwanshi, K.K. and Shukla, M.K. (2024) An Optimized Secure Cluster-Based Routing Protocol for IoT-Based WSN Structures in Smart Agriculture with Blockchain-Based Integrity Checking. *Peer-to-Peer Networking and Applications*, **17**, 2609-2636. https://doi.org/10.1007/s12083-024-01748-1

[148] Brickclay (2023) Future of AI and Machine Learning: Trends and Predictions. https://www.brickclay.com/blog/machine-learning/future-of-ai-and-machine-learning-trends-and-predictions/

[149] Dilmegani, C. (2024) Future of Deep Learning According to Top AI Experts of 2023. AI Multiple. https://research.aimultiple.com/future-of-deep-learning/