IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 January 2023, accepted 10 February 2023, date of publication 16 February 2023, date of current version 18 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3246180

TOPICAL REVIEW

A Review on the Security of IoT Networks: From Network Layer's Perspective

ASMA JAHANGEER[1], SIBGHAT ULLAH BAZAI[1], SAAD ASLAM[2], SHAH MARJAN[3], MUHAMMAD ANAS[1], AND SAYED HABIBULLAH HASHEMI[4]

[1]Department of Computer Science, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta 87300, Pakistan
[2]Department of Computing and Information Systems, School of Engineering and Technology, Sunway University, Selangor 47500, Malaysia
[3]Department of Software Engineering, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta 87300, Pakistan
[4]Department of Physics, Paktia University, Gardez, Paktia 2201, Afghanistan

Corresponding author: Sayed Habibullah Hashemi (hashami1984@gmail.com)

ABSTRACT Internet of Things (IoT) has revolutionized the world in the last decade. Today millions of devices are connected to each other utilizing IoT technology in one way or the other. With the significant growth in IoT devices, the provision of IoT security is imperative. Routing protocol for low power and lossy networks (RPL) is a network layer protocol, specially designed for routing in IoT devices. RPL protocol faces many attacks such as selective forwarding attacks, blackhole attacks, sybil attacks, wormhole attacks, and sinkhole attacks. All these attacks pose great threats to IoT networks and can substantially affect the performance of the network. In this work, a comprehensive review of internal attacks on the network layer is presented. Specifically, we focus on the literature that considers presenting solutions for the detection and prevention of sinkhole attacks. We reviewed the state-of-the-art works and different performance parameters like energy consumption, scalability, threshold value, packet delivery ratio, and throughput. Moreover, we also present a detailed analysis of machine learning-based algorithms and techniques proposed for the security of RPL protocol against internal attacks.

INDEX TERMS IoT, machine learning, network layer, RPL, sinkhole attack.

I. INTRODUCTION

Kevin Ashton presented the concept of the Internet of Things (IoT) for the 1st time in 1999 [1]. IoT is basically an idea of interconnected devices that can communicate, collect data from the environment, process data, and share collected data to achieve a particular goal. Today, IoT has enabled automation in all aspects of life, such as Smart Homes in the form of air conditioning, security surveillance, lighting, and many more countless services and devices. Moreover, other segments of human life have been impacted as well which led to Smart Education Systems, Smart Health Care, Smart Farming, Smart Industries, etc. It is estimated that the IoT industry will grow by 22 billion smart devices by the end of 2025 [2]. Therefore, it is important to investigate the challenges faced by IoT networks. Security is one of the main stumbling blocks for internet-connected devices. Since the invention of the Internet security attacks and threats have existed which are now expanding to IoT devices. Intruder activities can affect IoT devices in different ways [3], sometimes it overloads the traffic on the device with false consumers, and from time to time it causes network segment failure and sometimes exploits the network with eavesdropping. As the IoT networks got fame and IoT devices increased, attackers got busy challenging its security [4], [5]. There are many security issues that have appeared in the field of IoT. IoT is known as the heart of the 4th industrial revolution (4IR) [6], [7]. With this new trend different technologies are introduced such as virtualization, cloud computing, cyber-physical systems, and semantic web. These applications have also opened doors for attackers and they can potentially target the user and devices. The New York dam attack in 2013 is an important example where hackers got remote access to the dam system through a cellular modem and posed serious threats to the

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

system [8]. Norwegian company Norsk Hydro stopped its online production operations as the system was affected by ransomware in 2019 [9].

IoT architecture is mainly composed of three layers known as the perception layer, network layer, and application layer [10], [11], [12], [13]. Each layer has its own security challenges and attacks. For example, the perception layer faces cyber-physical attacks, eavesdropping, and RFID tracking attacks. Common attacks on network layer include Distributed denial of service (DDoS) attack where service is unavailable, replay attack where the attacker first manipulates the message and then reorder the message packet, and Man in the middle (MITM) attack while injection and malware are examples of application layer attacks [14].

Security of all the above-mentioned layers which are presented in Figure 1 is very important for the efficient functioning of IoT technologies. However, this research targets network layer security issues, risks, and threats.

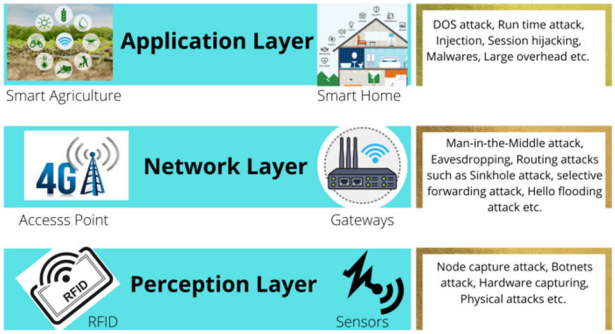

FIGURE 1. Security attacks on IOT layered architecture.

Most IoT devices are connected to Wireless Sensor Network (WSN) and have low battery power and less processing capabilities [15]. Routing Protocol for Low Power Lossy Network (RPL) is a network layer routing protocol which is especially designed for IoT technologies and now-a-days it is highly utilized in IoT devices [16]. RPL is a routing protocol for IPV6 header and also works with IEEE 802.15.4 standard. There are many attacks that RPL confronts internally and externally. Some of the attacks include selective forwarding attack, hello flooding attack, clone ID attack, sinkhole attack, black hole attack, rank attack, and many more. These attacks are presented in Figure 3. The security of RPL needs to be carefully considered. These attacks cause delays in data packets or complete loss of message packets, increased battery power consumption, and an intention for higher security risks for consumers and devices [17].

Taking into consideration the above discussion and realizing that network layer security is critical for IoT networks, this study investigates the current trends, and identifies the weakness of current schemes, while providing potential future directions for introducing more effective security techniques based on Machine Learning (ML) and otherwise.

The organization of the manuscript is as follows. Section II presents the detailed information on the IoT architecture, and security attacks on IoT devices. In section III relevant and recent literature is reviewed. Different performance parameters utilized for evaluating RPL security are discussed in section IV. In section V machine learning based solutions for securing IoT devices at the network layer are presented.

TABLE 1. List of acronyms.

ACRONYMS	DEFINITIONS
4IR	4th Industrial Revolution
AES	Advance Encryption Standard
AODV	Ad hoc on-demand Distance Vector
CFRs	Cumulative Forwarding Rates
CFS	Correlation-based Features Selection
CH	Cluster Head
COAP	Constrained Application Protocol
CSV	Comma Separated Value
DAG	Directed Acyclic Graph
DAO	Destination Advertisement Object
DCA-SF	Data Clustering Algorithm (DCA) for Detecting a Selective Forwarding Attack
DDoS	Distributed Denial of Service
DFW	Distributed Frank-Wolfe
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DL	DL Deep Learning
DODAG	Destination-Oriented Directed Acyclic Graph
DSR	Dynamic Source Routing
ECC	Elliptic curve cryptography
FBMM	Flow Based Mitigation Model
FNR	False Negative Rate
FPR	False Positive Rate
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IN	Inspector Node
IPV6	Internet Protocol Version 6
IoT	Internet of Things
KNN	K Nearest Neighbor
MDR	Missed Detection Rate
MITM	Man in the Middle
ML	Machine Learning
MNs	Member Nodes
MP2P	Multipoint to Point
NB-DPC	Noise-Based Density Peaks Clustering
MQTT	Message Queue Telemetry Transport
OF	Object Function
OSPF	Open Shortest Path First
OLSR	Optimized Link State Routing
P2MP	Point to multipoint
P2P	Point to Point
PASR	Prevention of an Active Sinkhole Routing Attack
PASH	Privacy-Aware Smart Health
PDR	Packet Delivery Ratio
RBF	Radial Basis Function
RRM	Route Request Message
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RL	Reinforcement Learning
SDN	Software Define Network
SN	Sink Node
SSL	Secure Socket Layer
SVM	Support Vector Machine
TNR	True Negative Rate
TPR	True Positive Rate
TEEN	Threshold Sensitive Energy Efficient Sensor Network
WPN	Wireless Personal Area Network
WSN	Wireless Sensor Network
XAMPP	Cross-platform, Apache, MySQL, PHP and Perl

In section VI future research directions are discussed and the conclusion is presented in Section VII.

II. IOT ARCHITECTURE, PROTOCOLS, AND ATTACKS

In this section, we provide details on different layers of the IoT architecture and discuss external attacks on this layered architecture. Moreover, protocols such as 6LoWPAN and RPL are discussed while providing details on different attacks on these protocols.

A. SECURITY ATTACKS ON THE LAYERED ARCHITECTURE OF IoT

1) ATTACKS ON THE PHYSICAL LAYER

The functionality of the physical layer is hampered by tampering, jamming, and spoofing. Attackers extract the information from sensors during the tampering attack using jamming techniques. Typically, a very high radio frequency is used to overpower the signals causing the SNR to decrease [18]. On the other hand, in spoofing attacks, forged identity information is embedded to destroy legitimate information. Spoofing is another threat to the physical layer that can occur during the transmission phase by introducing deceived signal [19], [20], [21].

2) ATTACKS ON THE NETWORK LAYER

The network layer is the target of many routing attacks due to the multi-hop environment. Sinkhole and selective forwarding are examples of routing attacks [22], [23]. These are discussed in detail in subsequent sections. DDoS occurs on this layer by spoofing and modifications in the routing path. Eavesdropping attacks are important to discuss as well since they put the security and privacy of the system at high risk. Important information about network nodes is obtained by the attacker through the eavesdropping method which impacts the quality of service (QoS). Most of the times eavesdropper targets insecure or weak network to access valuable or confidential data that may result in identity theft and financial loss.

3) ATTACKS ON THE APPLICATION LAYER

The application layer is vulnerable to different attacks as the end users can access network services directly which opens the gate for unauthorized and malicious users. MQTT, XAMPP, and COAP are widely used application layer protocols that are designed to protect against attacks but they are also vulnerable to security attacks. These attacks have a direct impact on the working of applications. DDoS, sniffing, malicious node injection and phishing attacks are the most common examples [23], [24].

B. 6LoWPAN

Internet engineering task force (IETF) defined 6LoWPAN as a standard that enables the use of IPV6. Most small and low-powered IoT devices use wireless personal area networks (WPAN). 6LoWPAN is a network layer protocol. It permits internet connection using open standards. In the beginning, it was difficult to implement IPV6 on IoT devices due to low energy constraints but 6LoWPAN overcame this issue and brought major changes in the use of this technology for IoT devices and networks. Mobility and scalability of the sensor network are increased by the 6LoWPAN [25]. There are many attacks and security threats that 6LoWPAN faces. Mainly these attacks are divisible on confidentiality, fragmentation, and authentication of data. Confidential data can be breached by man-in-the-middle attacks and eavesdropping. Different encryption mechanisms are used to secure the data for end-to-end communication by use of IPsec. When data is received in the form of fragments there is a possibility that fragmented data is spoofed, and an attacker can embed his own fragment in the chain. Moreover, authentication attacks can occur as IoT devices become part of network topology without proper authorization mechanisms. An optimal node authorization/authentication mechanism can be used to protect the network topology against such attacks [26].

C. RPL PROTOCOL

Most IoT devices today have low power and lossy networks so traditional routing like RIP, DSR, OSPF cannot be applied. Smart devices have constraints like limited memory and energy and less processing power, therefore, use RPL protocol for routing purposes. Initially, the RPL protocol relied on the directed acyclic graph (DAG) that introduced the problem of the routing loop (algorithm not converging to outgoing links). Therefore, destination-oriented DAG (DODAG) was introduced to help achieve a loop-free network, converging to a single destination [27]. Point-to-multipoint (P2MP), Multipoint to point (MP2P), and Point to point (P2P) are three types of traffic that RPL supports [28], [29]. The rank number is used to identify the position of each and every node in the DODAG graph. The rank number is also used to measure the node distance from the root node and to the neighbor's node [30]. There are three ways to categorize nodes in the RPL, which are described in Table 2.

TABLE 2. Categories of nodes in RPL.

Host	Router	LoWPAN Border Router (LBR)
End devices or leaf nodes are known as hosts.	Generation of traffic and message forwarding are the tasks of the router.	A border router, also known as sink node, or DODAG root.

The individual position of each node and its path from LBR is differentiated by rank for each node in the DODAG. Similar to node categorization, there are three types of main control messages [31], [32]. These messages are described below.

1) DODAG INFORMATION OBJECT (DIO) MESSAGE

DIO messages multicast to help other nodes discover the RPL instance to join [33].

2) DODAG INFORMATION SOLICITATION (DIS) MESSAGE

It is known as the link-local multicast and only requests for DIO neighbor discovery in the RPL instance [34].

3) DESTINATION ADVERTISEMENT OBJECT (DAO)

As its name suggests, DAO messages help to cover the distance in a network for bi-direction communication by constructing the routes for message flows from child nodes to the parent node or to the root node.

A node joins an RPL instance as a host by a pre-shared authentication key. If any node wants to join the RPL as a router then it is mandatory to obtain a secondary key from the key authority [35].

For traffic management, there are two types of DODAG route formation which are discussed as follows.

4) UPWARD ROUTE

DIO and DIS use an upward route specifically for MP2P type of traffic. Significant information like version, Instance ID, timer, and Object Function (OF) are carried by grounded nodes to calculate rank to its relevant neighbor [36]. DIO message is shared among nodes that want to join DODAG. If any node is interested it adds its address to the already created OF and updates the DIO message and multicasts it to other nodes in the neighbor [37]. DIO message is discarded by the nodes which are already part of the DODAG. In the case of floating nodes, DIS message is multicast to the nearest nodes. After receiving the message, floating node selects the preferred parent or neighbor by sending back a unicast DIO message. The representation of the upward route is shown in Figure 2.

5) DOWNWARD ROUTE

DAO messages use downward routes specifically for P2MP and P2P traffic. Neighbor discovery protocol is used here for route formation [38]. To maintain a downward route there are two types of modes that the RPL protocol follows, defined below.

Storing mode: In storing mode routing information is maintained by every router node.

Non-storing mode: In non-storing mode routing information is maintained by only the sink node and the sink node shares traffic information with other nodes.

In case of loop generation or failure between two nodes, a local repair scheme is performed with the help of the repair parent. But to reach the sink node optimal path is required which is not led by a local repair scheme therefore global repair scheme is used to find an optimal path where the DODAG version number is incremented which helps to construct a new DODAG with an optimal path. Figure 2 shows the concept of the RPL protocol.

D. ATTACKS ON RPL ROUTING PROTOCOL

There are many network attacks on RPL protocol because of the limitation of 6LoWPAN e.g. link failures, limited processing power, mobility, and change in network topology. Mainly Network layer attacks are classified as external attacks and internal attacks [39], [40]. A detailed discussion of these attacks is presented next and summarized in Figure 3.

1) HELLO FLOODING ATTACK

As the name represents, the "Hello" message is broadcast by the attacker initially. The attacker shows itself as a neighbor and has a strong routing metric. Generally, in RPL protocol DODAG information is advertised by DIO message. This attack impacts the network when selecting the link layer as the default route. This attack can be overcome by RPL local and global repair mechanisms, but if hello flooding attack is accompanied by other internal attacks then securely operating the network while maintaining its performance becomes extremely difficult [41].

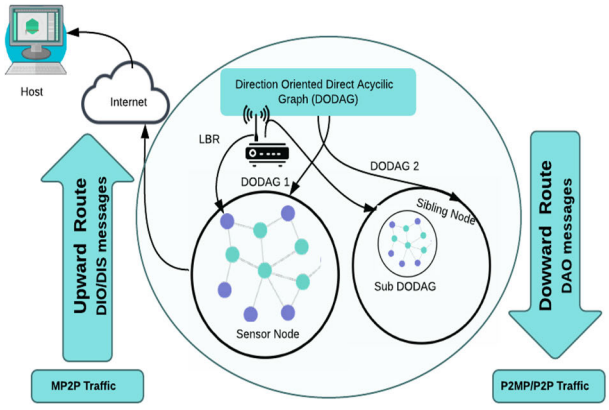

FIGURE 2. Concept of the RPL protocol.

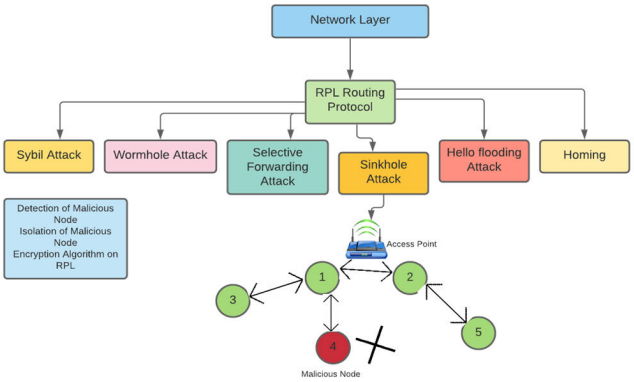

FIGURE 3. Attacks on RPL protocol.

2) CLONE ID ATTACK

An attacker can clone the identity of other nodes (also termed victim nodes). As a result, packets are misrouted by the attacker as they make multiple copies by acquiring the cryptographic secret and ID of the node. Typically, attacker nodes capture rank id and other related information of the nodes [42].

3) SELECTIVE FORWARDING ATTACK

This attack is launched by selectively forwarding the packets, which causes great disruptions in the routing path. DDoS can be enabled by this attack. Attackers drop all the traffic and only forward control messages [43].

4) SYBIL ATTACK

Several identities are used by the malicious node to take control of the network completely. It is similar to a clone id attack. In WSN because of the distributed environment, such attacks can easily be executed. The nodes that keep up the masquerade are known as Sybil node S and other nodes are known as normal nodes N. Sybil nodes adopt a new identity therefore it is considered misbehaving nodes causing confusion and collision in the network. The Sybil attack is divided into two forms. 1) Direct attack where Sybil node communicates directly with normal node. 2) Indirect attack where malicious node (an intermediate node) communicates with the normal node [44].

5) BLACKHOLE ATTACK

In a blockhole attack all the data packets which contain actual messages are dropped or blocked by the attacker node and messages with false information are forwarded which causes control overhead and packet delay. A node wanting to reach the destination is deceived by alluring into the shortest path toward the destination node. After receiving data packets instead of transferring them to the right destination, denial of service occurs and the packet is dropped and location exploitation can take place as well. This results in a lack of communication between real source and destination nodes. The blockhole node cannot be seen in the network, therefore it is required to observe the network traffic carefully. Blackhole attack causes network performance degradation such as reduced throughput, and routing issues [45].

6) SINKHOLE ATTACK

The sinkhole attack occurs when fake or compromised routing information is shared among the nodes. Each sensor node tries to find the shortest route by evaluating the rank for sending packets to the sink node. Any malicious node can change the rank artificially and shows a better route and better link availability. A legitimate node gets deceived by the attacker node advertisement showing a better route. It focuses on routing patterns and is considered an active attack. Sinkhole is created on a compromised node (CN) which attracts other nodes towards it and has a higher routing metric by which it is on higher precedence [46]. Sinkhole attacks when combined with other attacks overwhelm a larger network. A sinkhole attack is demonstrated in Figure 4. In the figure below node 1 is the source node and node 4 is the destination. For this to take place, there are many routes possible depicted by black dotted lines. Node 5 which can be seen in Figure 4 is a sinkhole node that offers much better routing costs and therefore attracts other nodes [47].

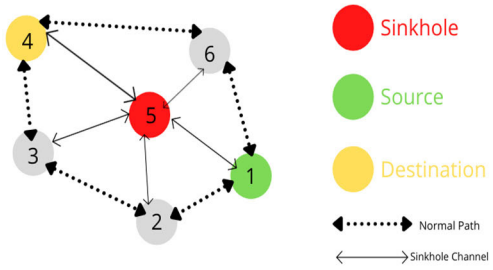

FIGURE 4. Sinkhole attack.

7) WORMHOLE ATTACK

Wormhole attacks can impact RPL protocol by creating disruption in traffic flow and network topology. In this attack, all the data packets, and traffic is routed via a tunnel created by two attackers. There are two ways in which a wormhole occurs. Encapsulation process, where the packet is received to the associated/neighbor node in encapsulated form and it is a detached packet from the payload. Packet relay is another way where malicious node relay packets to distant nodes perceived as neighbors [48], [49].

Based on the first two sections, the authors believe that the following research question (RQ) needs to be addressed to present the current state of security protocols used for IoT networks.

RQ1: How machine learning can be used to secure IoT applications against different attacks? Is there any algorithm or technique of ML that is used on the Network layer to secure against internal attacks such as sinkhole attack? A mind map of the research can be seen in Figure 5.

III. LITERATURE REVIEW

IoT is a vast field of study. It represents billions of small interconnected devices. These devices consist of limited resources such as energy, memory, and computational capability. These devices communicate by a low-power wireless standard known as 6LoWPAN. It allows devices to connect to the IPV6 network. It has been subjected to numerous attacks therefore a new protocol for routing in Low power and Lossy networks was introduced known as RPL. RPL also faced many internal and external attacks which are discussed in the literature section.

Figure 6 describes the criteria for selecting relevant and recent literature. First of all, selected keywords like IoT, machine learning, sinkhole attack, network layer, and RPL protocol are used to download recent papers between 2015-2022 for the research. All papers are from top Q1 journals and top-tier conferences. In total over one hundred articles were reviewed, out of which 83 references are cited in this manuscript comprised of 66 journals and 17 conference papers. A pictorial representation of the total number of studies considered in this work has can be seen in Figure 7. Figure 8 showcases a graphical representation of the work which is cited in this research. Moreover, Figure 8 also

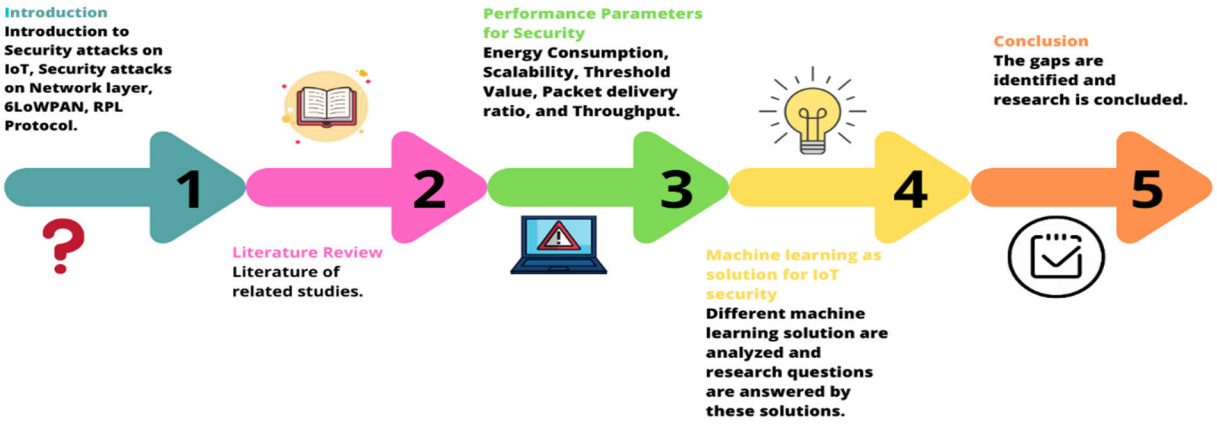

FIGURE 5. Mind map of the conducted research.

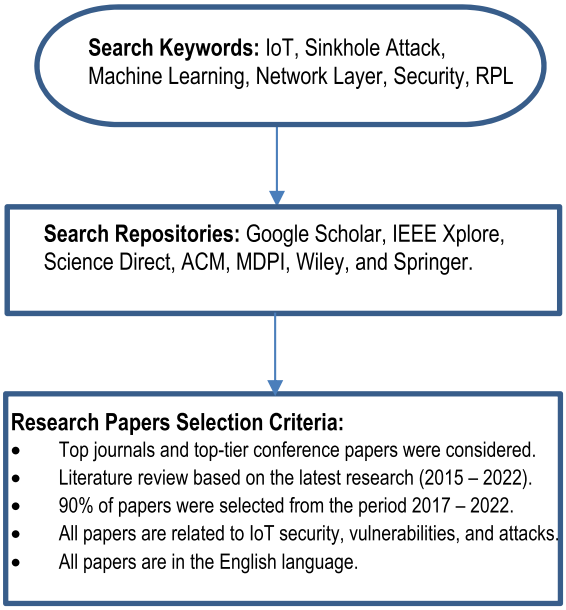

FIGURE 6. Criteria for paper selection.

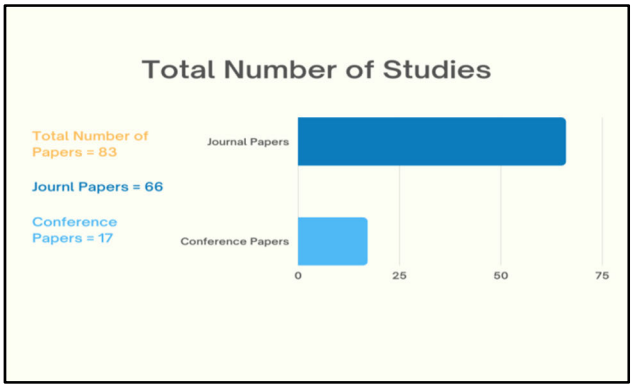

FIGURE 7. Distribution of considered studies.

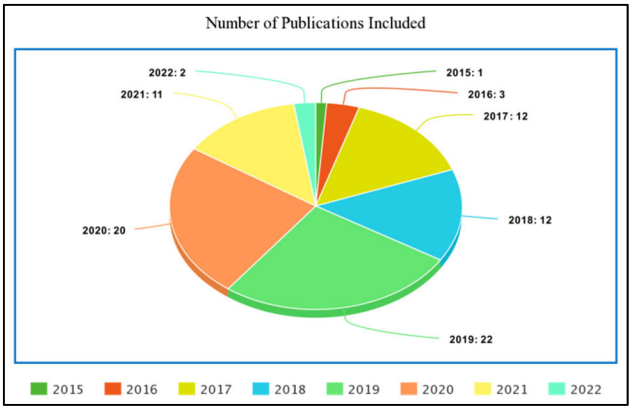

FIGURE 8. Publications selected from recent research.

summarizes the research works selected from each year during the 2015 – 2022 periods.

A. THE EXISTING APPROACH TO INTERNAL ATTACKS

In [50] the author discussed that IoT devices' security is different from traditional internet security therefore new and befitting encryption protocols and authentication processes are required. In the proposed method authors compare two encryption mechanisms AES (Advanced Encryption Standard with 128-bit) and PRESENT with 80-bit key. The authors believe that the PRESENT algorithm is lightweight and more suitable for RPL protocol.

1) CRYPTOGRAPHIC TOOLS FOR SECURITY

In [51] the author compared different solutions for the rank attack which represents one of the most threatening cyber-attack on RPL protocol. The rank attack causes energy consumption in nodes to increase and makes unnecessary topology changes. In RPL one particular node is selected as the parent node on the basis of its rank. This opens the door for the attacker to manipulate the ranks which compromises the network performance. Its solution is to use a unidirectional hash function (Cryptographic tools).

2) INTRUSION DETECTION SYSTEM FOR SECURITY

In [52] authors worked on the detection of two internal attacks namely; DIS and neighbor attack. In this work, Cooja was used for simulations and the dynamic threshold value was utilized to detect the attack. The proposed model worked on a lightweight Intrusion Detection System (IDS) which was distributed and worked stand-alone which means each node in the network monitors the neighbors and detects attacks. The performance of this detection system is evaluated by true positive rate (TPR) and false positive rate (FPR). The simulation results showed promising results for simulations running for short times but long runs deteriorate the performance of the proposed solution.

3) TRUST PATH SELECTION FOR SECURITY

The authors in [53] presented a two-stage security solution for selective forwarding attack and black hole attack. The performance of the network was evaluated via energy consumption. Data packets were divided into distributed routes so that the lifespan of the node can be increased. Elliptic curve cryptography (ECC) was used to encrypt each data packet before transmission. Malicious nodes were eliminated as only a trusted route was selected. The proposed method was evaluated against various performance parameters such as throughput, network size, latency, energy consumption, and packet drop ratio.

4) MULTI-LAYER SECURITY SYSTEM

In [54] author discussed the selective forwarding attack in military applications. Sensor nodes can detect activities on battlefield such as tank movement but a malicious node can destroy transmission and stop the packet from being transmitted. Multilayer detection for selective forwarding is proposed, detection layers include the MAC pool IDs layer, rule-based processing layer, and anomaly detection layer. NS-2 simulator is used for simulations and results were collected on basis of scalability, reliability, and energy efficiency.

5) FBSD MODEL FOR SECURITY

In [55] a model is presented to detect and mitigate sinkhole attack. FBSD-based mechanism is proposed where the first step is to log the generated traffic and secondly identify the transition path by traffic pattern discovery. In the third step snapshot of the topology is captured by taking different time variant snapshots. This work tried to address network latency, overhead increases, and sudden throughput decrease. The authors in [56] presented IDS based solution to detect the hybrid attack (Sink + Clone ID). A comparative study is presented to analyze the impact of standalone as well as hybrid i.e. combination of several attacks. Simulations are taken in Contiki OS using Cooja simulator. 6Mapper and power tracker are the modules that are used for the simulations. Power consumption and memory consumption results are compared for standalone attacks as well for Sink-Clone attack. It is concluded that a hybrid attack can be more destructive than a standalone therefore a more secure method is required for prevention.

6) PASR BASED SOLUTION FOR SECURITY

In [57] Detection and prevention of sinkhole attack is countered by introducing the prevention of an active sinkhole routing attack (PASR) based solution in which IoT clusters are built by network and connections are created between gateways and end devices. A sequence number is updated in the route request message (RRM) to activate the attack in ad hoc on-demand distance vector (AODV) protocol for testing purposes. Routing table is maintained by the gateways. Intrusion analyzer is used to detect anomalies in AODV protocol and broadcast messages to other gateways and base stations. This method performed well in terms of routing overhead, energy consumption, and packet delivery rate.

7) WATERMARKING FOR SECURITY

In [58] Sinkhole attack is detected on a prior basis before its activation by watermarking technique and homomorphic encryption algorithm. Threshold Sensitive Energy Efficient Sensor Network (TEEN) protocol is used for routing. Watermark is applied on each data packet for data authentication. Homomorphic encryption is used to ensure cluster node identity. For simulation purpose, OMNET++ is used.

8) IDS AND DIGITAL SIGNATURE BASED TECHNIQUE FOR SECURITY

In [59] authors proposed IDS and digital signature-based technique for detection and prevention of blackhole attack in MANETs. This research also developed a modified form of AODV protocol named as Detected blackhole AODV. According to this research, NS2 cannot detect AODV protocol if the protocol itself is attacked. Therefore, a modified version was introduced and different simulation runs were conducted with varying simulation time, packet size, and the number of nodes. Parameters like PDR, overhead, and delay were evaluated.

9) CROSS-LAYER DESIGN FRAMEWORK FOR SECURITY

In [60] Sinkhole attack in MANETs is detected by cross-layer design solution. Cross layers basically referred to different layers in a mobile network for efficient availability of network resources. It is proposed that for efficient transmission of packets, both security and QoS improvement are required. The cross-layer framework enables layers to communicate directly which eliminates the need for bandwidth optimization and helps in identifying fake routes. IDS is implemented with optimized link state routing (OSLR) which is a protocol for optimized link state routing. This work focused on improving the jitter, delay, and network throughput.

10) FUZZY RULE AND FEED FORWARD METHOD FOR SECURITY

In [61] author proposed a method for five routing attacks which are; Grayhole attack, Selective forwarding attack,

TABLE 3. Summary of the literature review.

Author and Year	Work Summary	Simulation Tool and Algorithm used	Limitations/Performance parameters				
			Energy Consumption	Scalability	Threshold value	Packet delivery ratio	Throughput
Alajmi et al. 2016	Selective forwarding attack on RPL is discussed for military applications. Multi-layer detection mechanism is purposed. [54]	NS-2 simulator	✓	✓	X	✓	✓
Devibala et al. 2017	This paper emphasis increasing the network performance by reducing the overhead in sinkhole attack. FBSD based solution is presented and snapshots of network are taken on different timeframes. Sinkhole attack is mitigated with the help of the physical features of the node. [55]	NS-2 simulator	X	X	X	✓	✓
Gawde et al. 2018	Comparison of AES and PRESENT algorithm. Suggests using PRESENT algorithm for IoT devices security in RPL protocol. [50]	PRESENT algorithm	X	X	X	X	X
Mehetre et al. 2018	Selective forwarding and black hole attack on RPL protocol are discussed. Two-stage solution ECC and trust path selection are purposed. [53]	Cuckoo search algorithm	✓	X	X	✓	X
Farzaneh et al. 2019	DIS attack and Neighbor attack on RPL protocol are discussed. Lightweight IDS is presented as solution. [52]	Cooja simulator	X	X	✓	X	X
Mirshahjafari et al. 2019	In this paper, hybrid attack (comprised of multiple attacks) is evaluated. It is observed that as the malicious traffic is increased, the network performance decreases. As RPL is highly propitious to attacks so more investigation is required covering hybrid attacks on RPL. [56]	Cooja simulator	✓	X	X	✓	X
Tahir et al. (2019)	PASR based solution is presented to detect sinkhole attack. In its implementation gateway devices are considered as cluster head and IoT network are divided into different clusters. Alert message is generated by the base station if an intruder enters the network. [57]	NS-2 simulator	✓	X	X	✓	X
Boudouaia et al. 2020	Rank attack of RPL protocol is discussed. IDS, Unidirectional hash function, Trust base detection, and identification scheme are compared. [51]	Friedman test	X	X	X	✓	X
Babaeer et al. (2020)	A novel approach is presented in this paper to detect sinkhole attack by watermarking techniques and use of lightweight encryption algorithm. Simulations are performed in OMNT++. Parameters like energy consumption, throughput, packet delivery ratio and delay are considered. [58]	OMNET++	✓	X	X	✓	✓
Talukdar et al.(2021)	Digital signature based encryption technique along with IDS is proposed for detection and mitigation of blackhole attack from MANETs. AODV protocol in MANETs is implemented with BH-AODV and D-B-AODV. NS2 is used for simulation. [59]	NS-2 simulator	X	X	X	✓	X
Esiefarienrhe et al. (2022)	Sinkhole attack detection is performed in MANETs by providing a security framework. Three steps implementations involve; sinkhole attack, IDS design by using OLSR and lastly proposing framework for security. [60]	Netsim	X	X	X	✓	✓
M. Ezhilarasi et al. (2022)	Different internal attacks are detected by using fuzzy rules and feed-forward neural networks. Packet delivery ratio, round trip time, and residual energy are analyzed. For experimental purpose, NS2 is used. [61]	NS-2 simulator	✓	X	X	✓	X

Sinkhole attack, Blackhole, and Wormhole attacks. The purpose of this paper is to detect all the above attacks by one method which is the fuzzy rule and feed-forward neural network. The authors also compared the proposed solution with traditional ML approaches such as RF, DT, and SVM. AODV protocol is used and residual energy, packet delivery ratio and trip times are selected features for performance analysis. Comparison is reported between the proposed method and other ML-based approaches e.g. SVM, RF, and DT. It is observed that computational complexity is very high that requires substantial resources. Hence, further investigation is required to address this problem.

The literature review is summarized in Table 3 which highlights the simulation tools used and performance parameters considered by each study. The summary of each research work is provided in the table as well.

IV. PERFORMANCE PARAMETERS FOR RPL SECURITY EVALUATION

A. ENERGY CONSUMPTION

Many IoT applications have limited energy so analysis of energy consumption is important. Network lifespan and lifespan of a single node in a network depend on energy consumption. Sending data packets to the sink node for optimizing throughput causes increased energy consumption which affects other parameters of the network [62]. While the size and frequency of data transmission impact energy consumption, network density also affect it. If data packets are lost, retransmission causes higher energy consumption as well [63]. Sinkhole attacks can be identified by analyzing energy consumption in the network and improved security solutions can be provided by minimizing energy consumption in the network. Trickle timer is used to minimize energy consumption and control messages in RPL. A lot of work has already been done in this aspect. In [64] a comparative study has been presented and the following Eq.1 is derived to calculate energy consumption in general.

$$E = E_{net} + E_{over} + E_{ids} \tag{1}$$

where;

$Enet = Network\ Energy$
$Eover = Overhead\ Energy$
$Eids = Execution\ energy\ of\ IDS$

B. SCALABILITY

The level of scalability is determined by the increment in the number of sensors/nodes in the network. Factors such as range and nodes' power impact the scalability. The scalability of the network can be analyzed under normal circumstances as well as for sinkhole compromised network. In [65], the performance of the sensor network is analyzed with respect to stability, and different parameters like packet delivery ratio, throughput, and jitter are used to analyze the network. Simulation results show that the delivery ratio and throughput decrease when the size of the network is increased while undergoing a sinkhole attack.

C. THRESHOLD

The threshold value can also help in identifying the sinkhole attack. In [66] threshold value is used to detect different attacks on RPL. For every node in the network, a dynamic threshold value is assigned. To calculate the threshold value, the following formula is used.

$$Threshold = \mu + k\sigma \tag{2}$$

In this equation μ is the average, k is the coefficient which determines the distance and σ is the standard deviation.

D. PACKET DELIVERY RATIO

Packet Delivery Ratio (PDR) is defined as the number of packets received at the destination to the ratio of packets sent by the source. PDR is calculated in percentage. When a sinkhole attack occurs, the PDR of the network is decreased as the sinkhole holds the packets affecting the overall network performance. In [67] comparison is done to analyze the effect of sinkhole attacks. It is observed that the PDR is high in the absence of the sinkhole and decreases as the attack occurs which indicates fluctuation in the network performance.

E. THROUGHPUT

The performance of a network is indicated by throughput because it measures the actual number of packets that are delivered per second. Mostly throughput is measured by the number of bits transferred per second. Low throughput creates many problems and it can be an indication of a sinkhole attack. During the sinkhole attack, many nodes select the same path which increases traffic and causes latency [68]. As a result, throughput is decreased. Therefore, we need mechanisms that can keep the throughput of the network above a given value even when the network is undergoing a sinkhole attack.

V. IoT SECURITY FROM THE MACHINE LEARNING PERSPECTIVE

Machine learning (ML) has revolutionized the field of IoT and how it can be a solution to security problems. Different ML algorithms help industries and businesses to grow by identifying patterns. The task of ML is to learn from model behavior and utilize these models for either classification or future predictions. This is done independently without human intervention [69].

In [70] a systematic comprehensive survey of ML and deep learning (DL) is presented pertaining to IoT devices. In this survey, the authors discuss the applicability of ML to IoT devices. IoT devices are resource constraint as they have limited processing power and energy so ML cannot be directly implemented into IoT devices. On the other hand, IoT devices generate heterogeneous data and pre-processing is required since ML may not be able to process this data directly. In this survey, it is also emphasized that a mechanism is required to ensure user authentication so that the right person acquires the right data. Different ML, DL, and Reinforcement

learning (RL) based authentication and access control solutions are presented.

It can be observed from the literature [70], [71] that while ML offers unique security solutions for IoT networks, there is still a lot of pending research problems that need to be investigated. A summary of recent literature utilizing ML for detecting internal attacks has been presented in Table 3.

A. MULTI-LEVEL FRAMEWORK

In [72] a multi-level framework is proposed for the mitigation of DDoS. These multi-levels consist of edge, fog, and cloud computing. Software Defined Networking (SDN) is used with gateways at the edge and then honeypots are used with SDN controller to collect data traffic at fog and this collected data is analyzed for mitigation of DDoS attack. In [73] the authors used an ML approach for the detection and avoidance of DDoS where four steps are followed for anomaly detection in the network. These four steps include traffic capturing, packet grouping by device and time, feature extraction, and binary classification. For testing purposes, the authors have collected consumer IoT devices and applied five ML classifiers namely KNN, SVM, Decision Trees (DT), Random Forest (RF), and Neural Networks (NN). Promising results are reported by this study.

The authors in [74] review different attacks like jamming, spoofing, eavesdropping, and denial of service. The ability of ML techniques to detect these attacks is discussed as well. From the literature, it can be observed that it is critical to identify the attack at the beginning but traditional ML schemes have not been able to do this even with the multilayer framework. Moreover, traditional ML techniques have high implementation cost in terms of communication and computation, therefore low-cost solutions need to be investigated for IoT security systems.

B. HOST/WWWWW/NETWORK BASED ML TECHNIQUE

The authors in [75] proposed a solution for IoT device security utilizing host and network-based ML techniques. Challenges while applying these techniques are discussed in detail. Limited hardware resources, connectivity, and heterogeneity are challenges of IoT devices. While applying a network-based defensive approach there are no restrictions on computational resources. By measuring the round trip time between incoming and outgoing packets reroute packets can be detected by IDS. Malicious traffic can be identified by using KNN or SVM as they are resource efficient and can use the same model many times for the detection of attack.

For host and network-based data collections, it should be noted that connectivity issues may result in missing data, therefore model accuracy can be affected. When IoT devices change state, they cannot be utilized with full potential. Malicious activity can be separated from normal ones by clustering in unsupervised learning. However, the computationally intensive nature of unsupervised learning algorithms makes it harder to analyze the data. In host-based supervised learning, spoofing attacks, malware, and intrusion attacks can be detected by ML (specifically utilizing SVM, and KNN). As the host interacts with other network devices, traffic classification can take place.

C. CHA-IDS BASED ML TECHNIQUE

The authors in [76] worked on the 6LoWPAN protocol and detected the combined and individual routing attacks by Compression Header Analyzer – Intrusion Detection System (CHA-IDS). Raw data is collected and analyzed, and based on the analysis appropriate actions are taken making a framework of a multi-agent system. For intrusion detection systems, correlation-based significant features are selected which are then used to differentiate normal and attack scenarios. The impact of wormhole, sinkhole, and hello flooding attacks are determined in terms of memory consumption, accuracy of detection, and energy consumption. In the first layer, which is a sensor agent, a cooja traffic analyzer is used to collect packets. The second layer is the aggregator agent which is responsible for finding significant features by using Correlation-based Features Selection (CFS) algorithm. Third layer represents the analyzer agent in which WEKA tool is used to compare ML algorithms. The fourth layer is the actuator agent in which threshold value is compared and if it is exceeded, an alert is given to the user. Tmote Sky is used as an IoT device to calculate memory and energy consumption.

D. CLUSTERING ALGORITHM DCA-SF AND NB-DPC

The authors in [77] and [78] proposed a data clustering algorithm (DCA) and a Noise-Based Density Peaks Clustering (NB-DPC) algorithm for detecting a selective forwarding attack (DCA-SF). In cluster-based selective forwarding attack, cluster heads (CH) is compromised which disconnects form some or all of its cluster members. In this work, it is suggested that by clustering cumulative forwarding rates (CFRs) a malicious CH can be captured and isolated from the network. The detection mechanism consists of a cluster which has three nodes namely CH, inspector node (IN), and the member nodes (MNs). CH receives data packets from MN which consist of environmental information. This information is further transmitted to sink nodes (SN). CFR of CH and MN are calculated and depending upon calculations of the highest residual energy from IN, a particular MN becomes the new CH. Centralized and distributed are the two schemes that fall under DCA-SF category. In the case of a centralized scheme, after receiving CFR of all the CHs, DP-DBSCAN is independently executed, while in distributed detection scheme to confirm if a particular CH is malicious, IN performs DP-DBSCAN.

E. E-PASH SYBILWATCH APPROACH

A novel algorithm known as SybilWatch based on BlueTits Detection (BTD) algorithm for Sybil attack detection is presented in [79]. This algorithm addresses the issues of tractability of nodes and revocation.

Another study pointed out that the attacks on social media can be categorized as Sybil attacks [80]. As we all know that Twitter is one of the largest and fastest growing social media platforms with 317 million active users from all over the globe, therefore more prevailed to attacks. Traditional detection techniques are no longer applicable to protect against Sybil attacks owing to the scale of the network as there are many organizations and individuals which can harm social media sites by increasing the fake number of followers. The research presented in [80], evaluated and analyzed user profiles on Twitter by a deep regression model and detected Sybil attack. Three integrated modules are proposed in their works, described below.

1) DATA HARVESTING MODULE

Data harvesting module in which 5000 user IDs are utilized for gathering information like the number of posts, trending metrics, etc.

2) FEATURE EXTRACTING MECHANISM

Feature extracting mechanisms in which profile, content, and graph-based features of users are extracted by Twitter API, in total 80 online-offline features were extracted.

3) DEEP REGRESSION MODEL

A prediction system is introduced which recognized activity patterns of Sybil profiles on basis of user characteristics User who uses the English language on Twitter, their accounts are taken as database and the trustworthiness of Sybil node is predicted. A malicious Sybil node sends a friend request to other nodes in the network, the purpose of this is to detect the colluded node by regression model not only in government agenesis but also in private enterprises and for individual security.

F. GINI INDEX-BASED COUNTERMEASURE

It is important to observe the energy consumption of nodes and special attention is being paid if multiple devices/nodes lose energy at once. During the Sybil attack, multiple DIS messages are sent that can cause fast depletion in energy. In [81], Sybil attack is detected and mitigated by GINI index-based countermeasure. To measure the dispersity in the DIS message a GINI impurity is used. An excessive number of DIS messages point towards the abnormal range which influences the identities of GINI impurity and confirms the Sybil attack. While on the other hand if there exists no attack a stable distribution is maintained. After the detection of Sybil attack, DIO messages are minimized and an adaptive replaying rate of DIO messages is determined. An alert packet is constructed and broadcasted to the nearest nodes, by the node which detects the Sybil attack.

The authors in [82] considered Minimum Rank with Hysteresis Object Function (MRHOF) to detect hybrid attacks and analyze vulnerabilities. To enhance security, RF and MLP-based machine learning approaches were used. For the creation of dataset, different private and publicly available datasets were explored.

G. AI-BASED FRAMEWORK

The authors in [83] discussed the inability of conventional techniques to handle novel attacks like clone ID in RPL networks for IoT devices. A framework based on AI is proposed to cater to such kinds of attacks. The selection of the key characteristics from RPL is categorized by unsupervised pre-training technique.

Conventionally, IDS/IPS provided continuous network observation that leads to many problems like resource and time consumption. In a clone ID attack, identities are impersonated by legitimate nodes. An attacker can directly leak, alter, ex-filtrate, and spoof the data coming from the clone root node.

To apply the new technique proposed in [83], real-time traffic data was gathered consisting of normal and malicious nodes. A supervised learning approach was used where a DNN model with one outer layer and two hidden layers was adopted. This DNN model helped in recognizing network communication with impersonated nodes.

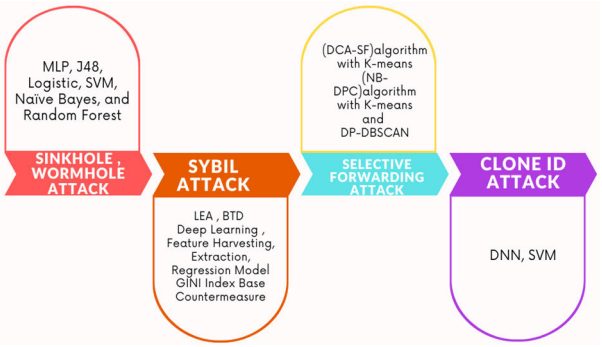

FIGURE 9. Commonly used ML algorithms and techniques for detecting security attacks.

VI. FUTURE RESEARCH DIRECTIONS

From the detailed literature review and the summary presented in Tables 3 and 4, it is evident that RPL security is of paramount importance. There are several works reported in this area, however, gaps can be identified that need researchers' attention.

Firstly, it is important to understand that different attacks on RPL can cause different network parameters to report faulty values. Therefore, to detect security attacks not only selected parameters rather most of the parameters need to be analyzed. This will give a better and bigger picture required to detect attacks.

Secondly, an extensive body of work can be found that utilizes ML for improving the performance of the network however, when it comes to detecting security attacks, ML is still underutilized. Moreover, a unified approach to implementing ML for resource-constraint IoT devices needs to be investigated and designed. The recent literature suggests that

TABLE 4. A summary of machine learning approaches for detecting internal attacks on the network layer.

S.#	Reference	Year of Publication	Attacks Covered	Machine Learning Approaches/Algorithm
1	Napiah et al.[76]	2018	Sinkhole, wormhole, and hello flooding attack	MLP, J48, Logistic, SVM, Naïve Bayes, and Random Forest.
2	Fu et al.[77]	2020	Selective forwarding attack	(DCA-SF) algorithm compared with K-means.
3	Ding et al.[78]	2021	Selective forwarding attack	(NB-DPC) algorithm compared with K-means and DP-DBSCAN.
4	Vaishnavi et al. [79]	2020	Sybil attack	LEA algorithm and BTD algorithm.
5	Al-Qurishi et al.[80]	2018	Sybil attack	Deep learning solution, feature harvesting, extraction and regression model.
6	Groves et al.[81]	2019	Sybil attack	GINI index base countermeasure.
7	Foley et al. [82]	2020	Combine attacks (Sybil attack, blackhole attack, decreased path attack, and version attack)	RF, MLP, NB, SVM, and ZeroR
8	Morales-Molina et al.[83]	2021	Clone ID attack	DNN

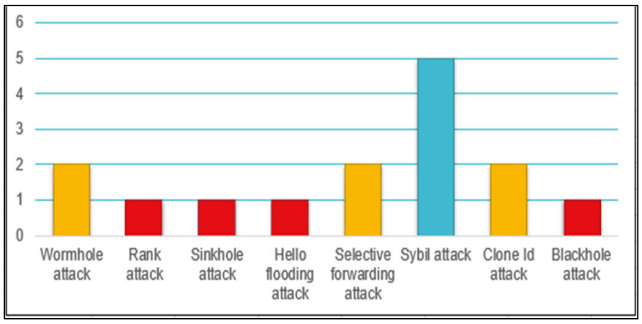

FIGURE 10. Graphical representation of ML-based solution covered in this research.

ML approaches are yet to focus on detecting internal attacks. A mechanism is required where RPL protocol can be secured not only from the sinkhole attack but also from other internal attacks as well. Most importantly such mechanisms should ideally be distributed in nature and their implementation should not derail the performance of the IoT network.

Thirdly, more investigation is required to secure IoT devices at the network layer. It should be noted that on-device security solutions are very limited for IoT networks therefore devices such as routers, switches, and firewalls can be subjected to Spoofing and DDoS attacks and thus require new and improved security mechanisms. It is significant since hardware or device-level attacks can go undetected by the software.

To secure the network layer, attacks on RPL, or more generally, to secure the IoT network, a layered security approach is required. It represents designing layer-specific software by layer-specific specialists. Mostly, an IT specialist is given the role of handling network security aided by certain hardware and software tools. Rather, a distributed approach is required where each layer is dealt with by a specialist (i.e. a network layer specialist) using layer-specific tools.

VII. CONCLUSION

Technology advancement has brought the risk of cyber-crimes for IoT networks. With the significant increase in the deployment of IoT networks, it has become necessary to understand the current state of security protocols for IoT networks. Keeping this in view, this manuscript presented a comprehensive review of the external and internal security attacks on IoT devices. Details on the layered structure of IoT are presented as well. Moreover, protocols especially designed for IoT devices are discussed in detail. It is found, to protect the network layer against internal attacks different performance parameters are required to be analyzed. Once the network security is breached it impacts various performance parameters such as energy consumption, throughput, packet delivery ratio, etc. It is believed that ML has made enough progress to present solutions for protecting IoT devices against security attacks. Currently, ML is more focused on detecting external attacks and a thorough investigation is required for internal attacks as well. It is observed that the nature of the IoT network is an obstacle when designing security protocols. IoT network is mostly comprised of sensors having limited capabilities therefore, it is challenging to implement robust and computationally complex algorithms. The RPL protocol does not have a pre-defined standard for its security operation, therefore researchers need to standardize the security implementation protocol.

REFERENCES

[1] T. P. Nguyen, G. N. Pham, and B. A. Nguyen, "Internet of Things: Introduction communication models technologies applications and open-issues," *Int. J. Res. Publication Rev.*, vol. 2, no. 12, pp. 1303–1312, 2021.
[2] T. Sanislav, G. D. Mois, S. Zeadally, and S. C. Folea, "Energy harvesting techniques for Internet of Things (IoT)," *IEEE Access*, vol. 9, pp. 39530–39549, 2021.
[3] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2018.
[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[5] B. Schneier, "IoT security: What's plan B?" *IEEE Secur. Privacy*, vol. 15, no. 5, p. 96, Sep. 2017.

[6] S. Biller, "The operational butterfly effect: How IoT data + AI help deliver on the promise of 4IR," in *Proc. IEEE 15th Int. Conf. Autom. Sci. Eng. (CASE)*, Aug. 2019, p. 1.

[7] S.-W. Lee, J. Jo, and S. Kim, "Leveraging the 4th industrial revolution technology for sustainable development of the Northern Sea Route (NSR)—The case study of autonomous vessel," *Sustainability*, vol. 13, no. 15, p. 8211, Jul. 2021.

[8] S. E. Chandy, A. Rasekh, Z. A. Barker, and M. E. Shafiee, "Cyberattack detection using deep generative models with variational inference," *J. Water Resour. Planning Manage.*, vol. 145, no. 2, Feb. 2018, Art. no. 04018093.

[9] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, pp. 1–20, 2020.

[10] S. G. Abbas, F. Hashmat, and G. A. Shah, "A multi-layer industrial-IoT attack taxonomy: Layers, dimensions, techniques and application," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1820–1825.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[12] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[13] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A self organizing map intrusion detection system for RPL protocol attacks," *Int. J. Interdiscipl. Telecommun. Netw.*, vol. 11, no. 1, pp. 30–43, Jan. 2019.

[14] H. F. Atlam and G. B. Wills, *IoT Security, Privacy, Safety and Ethics*. Cham, Switzerland: Springer, 2020.

[15] S. Y. Hashemi and F. S. Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *J. Supercomput.*, vol. 75, no. 7, pp. 3555–3584, Jul. 2019.

[16] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schonwalder, "Using the RPL protocol for supporting passive monitoring in the Internet of Things," in *Proc. IEEE/IFIP Netw. Operations Manage. Symp. (NOMS)*, Apr. 2016, pp. 366–374.

[17] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Jun. 2017, doi: 10.1109/JIOT.2017.2749883.

[18] Y. Al-Hadhrami and F. K. Hussain, "DDoS attacks in IoT networks: A comprehensive systematic literature review," *World Wide Web*, vol. 24, no. 3, pp. 971–1001, May 2021.

[19] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[20] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[21] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[22] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, Oct. 2019, Art. no. 100179.

[23] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018.

[24] L. Nastase, "Security in the Internet of Things: A survey on application layer protocols," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2017, pp. 659–666.

[25] Y. Qiu and M. Ma, "Secure group mobility support for 6 LoWPAN networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1131–1141, Apr. 2018.

[26] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Netw.*, vol. 82, pp. 100–112, Jan. 2019.

[27] A. E. Hassani, A. Sahel, A. Badri, and E. M. Ilham, "A hybrid objective function with empirical stability aware to improve RPL for IoT applications," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 3, pp. 2350–2359, 2021.

[28] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "Attestation-enabled secure and scalable routing protocol for IoT networks," *Ad Hoc Netw.*, vol. 98, pp. 1–14, Mar. 2020.

[29] M. Zhao, A. Kumar, P. H. J. Chong, and R. Lu, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities," *Peer-Peer Netw. Appl.*, vol. 10, no. 5, pp. 1232–1256, Sep. 2017.

[30] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, "Detection and mitigation of RPL rank and version number attacks in the Internet of Things: SRPL-RP," *Sensors*, vol. 20, no. 21, pp. 1–25, 2020.

[31] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a secure RPL based Internet of Things routing protocol: A review," *Ad Hoc Netw.*, vol. 101, Apr. 2020, Art. no. 102096.

[32] W. Khallef, M. Molnar, A. Benslimane, and S. Durand, "Multiple constrained QoS routing with RPL," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[33] C. Pu, "Spam DIS attack against routing protocol in the Internet of Things," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 73–77.

[34] C. Pu, "Sybil attack in RPL-based Internet of Things: Analysis and defenses," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4937–4949, Jun. 2020.

[35] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's Internet of Things Networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, 2019.

[36] H.-S. Kim, H. Cho, H. Kim, and S. Bahk, "DT-RPL: Diverse bidirectional traffic delivery through RPL routing protocol in low power and lossy networks," *Comput. Netw.*, vol. 126, pp. 150–161, Oct. 2017.

[37] H. Kharrufa, H. Al-Kashoash, Y. Al-Nidawi, M. Q. Mosquera, and A. H. KEMP, "Dynamic RPL for multi-hop routing in IoT applications," in *Proc. 13th Annu. Conf. Wireless Demand Netw. Syst. Services (WONS)*, Feb. 2017, pp. 100–103.

[38] I. Zaatouri, N. Alyaoui, A. B. Guiloufi, and A. Kachouri, "Performance evaluation of RPL objective functions for multi-sink," in *Proc. 18th Int. Conf. Sci. Techn. Autom. Control Comput. Eng. (STA)*, Dec. 2017, pp. 661–665.

[39] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in *Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT)*, Apr. 2019, pp. 28–33.

[40] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, "Trust-based attack and defense in wireless sensor networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–20, Sep. 2020.

[41] S. Cakir, S. Toklu, and N. Yalcin, "RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning," *IEEE Access*, vol. 8, pp. 183678–183689, 2020.

[42] S. R. Taghanaki, S. B. Arzandeh, and A. Bohlooli, "A decentralized method for detecting clone ID attacks on the Internet of Things," in *Proc. 5th Int. Conf. Internet Things Appl. (IoT)*, May 2021.

[43] Q. Zhang and W. Zhang, "Accurate detection of selective forwarding attack in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, Jan. 2019, Art. no. 155014771882400.

[44] C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. H. Anajemba, and A. K. Bashir, "On detection of Sybil attack in large-scale VANETs using spider-monkey technique," *IEEE Access*, vol. 6, pp. 47258–47267, 2018.

[45] M. B. Yassein, I. Hmeidi, Y. Khamayseh, M. Al-Rousan, and D. Arrabi, "Black hole attack security issues, challenges & solution in MANET," in *Proc. Conf.*, Apr. 2019, pp. 199–207.

[46] Y. X. Liu, M. Ma, X. Liu, N. N. Xiong, A. F. Liu, and Y. Zhu, "Design and analysis of probing route to defense sink-hole attacks for Internet of Things security," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 356–372, Jan./Feb. 2020.

[47] R. K. Sundararajan and U. Arumugam, "Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor networks," *J. Sensors*, vol. 2015, pp. 1–12, Feb. 2015.

[48] N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs," in *Proc. 9th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Jul. 2016, pp. 103–109.

[49] O. R. Ahutu and H. El-Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020.

[50] A. Gawde, N. Sakariya, A. Shah, and D. Poojary, "Lightweight authentication and encryption mechanism in routing protocol for low power and lossy networks (RPL)," in *Proc. 2nd Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Jun. 2018, pp. 226–229.
[51] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa, and P. Lorenz, "Security against rank attack in RPL protocol," *IEEE Netw.*, vol. 34, no. 4, pp. 133–139, Jul. 2020.
[52] B. Farzaneh, M. A. Montazeri, and S. Jamali, "An anomaly-based IDS for detecting attacks in RPL-based Internet of Things," in *Proc. 5th Int. Conf. Web Res. (ICWR)*, Apr. 2019, pp. 61–66.
[53] D. C. Mehetre, S. E. Roslin, and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust," *Cluster Comput.*, vol. 22, no. S1, pp. 1313–1328, Jan. 2019.
[54] N. M. Alajmi and K. Elleithy, "A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, Apr. 2016, pp. 1–6.
[55] K. Devibala, S. Balamurali, A. Ayyasamy, and M. Archana, "Flow based mitigation model for sinkhole attack in wireless sensor networks using time-variant snapshot," *Int. J. Adv. Comput. Electron. Eng.*, vol. 2, no. 5, pp. 14–21, 2017.
[56] S. M. H. Mirshahjafari and B. S. Ghahfarokhi, "Sinkhole+CloneID: A hybrid attack on RPL performance and detection method," *Inf. Secur. J., A Global Perspective*, vol. 28, nos. 4–5, pp. 107–119, Sep. 2019.
[57] S. Tahir, S. T. Bakhsh, and R. A. Alsemmeari, "An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 11, Nov. 2019, Art. no. 155014771988990.
[58] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and Secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking," *IEEE Access*, vol. 8, pp. 92098–92109, 2020.
[59] M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, and A. S. Ahmed, "Performance improvements of AODV by black hole attack detection using IDS and digital signature," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Mar. 2021.
[60] B. M. Esiefarienrhe, T. Phakathi, and F. Lugayizi, "Node-based QoS-aware security framework for sinkhole attacks in mobile ad-hoc networks," *Telecom*, vol. 3, no. 3, pp. 407–432, Jun. 2022.
[61] M. Ezhilarasi, L. Gnanaprasanambikai, A. Kousalya, and M. Shanmugapriya, "A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks," *Soft Comput.*, vol. 7, pp. 1–12, Mar. 2022.
[62] H. Bouzebiba and M. Lehsaini, "FreeBW-RPL: A new RPL protocol objective function for Internet of multimedia things," *Wireless Pers. Commun.*, vol. 112, no. 2, pp. 1003–1023, May 2020.
[63] H. Kharrufa, H. Al-Kashoash, and A. H. Kemp, "A game theoretic optimization of RPL for mobile Internet of Things applications," *IEEE Sensors J.*, vol. 18, no. 6, pp. 2520–2530, Mar. 2018.
[64] P. Bhale, S. Dey, S. Biswas, and S. Nandi, "Energy efficient approach to detect sinkhole attack using roving IDS in 6 LoWPAN network," in *Innovations for Community Services* (Communications in Computer and Information Science), vol. 1139. Cham, Switzerland: Springer, Dec. 2020, pp. 187–207.
[65] R. Baskar, P. C. K. Raja, M. Reji, and C. Joseph, "Performance analysis of scalability in WSN-sinkhole attack scenario," *Int. J. Pure Appl. Math.*, vol. 117, no. 9, pp. 35–39, 2017.
[66] A. I. Abdalla Ahmed, A. Gani, S. H. Ab Hamid, S. Khan, N. Guizani, and K. Ko, "Intersection-based distance and traffic-aware routing (IDTAR) protocol for smart vehicular communication," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 489–493.
[67] A. Arış, S. B. Ö. Yalçın, and S. F. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," *Ad Hoc Netw.*, vol. 85, pp. 81–91, Mar. 2019.
[68] X. Wei, T. Wang, and C. Tang, "Throughput analysis of smart buildings-oriented wireless networks under jamming attacks," *Mobile Netw. Appl.*, vol. 26, no. 4, pp. 1440–1448, Aug. 2021.
[69] D. Gunduz, P. de Kerret, N. Sidiroupoulos, D. Gesbert, C. Murthy, and M. Van Der Schaar, "Machine learning in the air," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 10, pp. 2184–2199, Oct. 2019.
[70] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.
[71] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *Proc. 18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jul. 2017, pp. 1–10.
[72] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018.
[73] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2018, pp. 29–35.
[74] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning," 2018, *arXiv:1801.06275*.
[75] S. Zeadally and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," *Int. J. Commun. Syst.*, vol. 33, no. 1, pp. 1–16, Jan. 2020.
[76] M. N. Napiah, M. Y. I. Bin Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (CHA–IDS) for 6 LoWPAN communication protocol," *IEEE Access*, vol. 6, pp. 16623–16638, 2018.
[77] H. Fu, Y. Liu, Z. Dong, and Y. Wu, "A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks," *Sensors*, vol. 20, no. 1, p. 23, Dec. 2019.
[78] J. Ding, H. Zhang, Z. Guo, and Y. Wu, "The DPC-based scheme for detecting selective forwarding in clustered wireless sensor networks," *IEEE Access*, vol. 9, pp. 20954–20967, 2021.
[79] S. Vaishnavi and T. Sethukarasi, "SybilWatch: A novel approach to detect Sybil attack in IoT based smart health care," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 6, pp. 6199–6213, 2021.
[80] M. Al-Qurishi, M. Alrubaian, S. M. M. Rahman, A. Alamri, and M. M. Hassan, "A prediction system of Sybil attack in social network using deep-regression model," *Future Gener. Comput. Syst.*, vol. 87, pp. 743–753, Oct. 2018.
[81] B. Groves and C. Pu, "A Gini index-based countermeasure against sybil attack in the Internet of Things," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2019, pp. 1–6.
[82] J. Foley, N. Moradpoor, and H. Ochenyi, "Employing a machine learning approach to detect combined Internet of Things attacks against two objective functions using a novel dataset," *Secur. Commun. Netw.*, vol. 2020, pp. 1–17, Feb. 2020.
[83] C. D. Morales-Molina, A. Hernandez-Suarez, G. Sanchez-Perez, L. K. Toscano-Medina, H. Perez-Meana, J. Olivares-Mercado, J. Portillo-Portillo, V. Sanchez, and L. J. Garcia-Villalba, "A dense neural network approach for detecting clone ID attacks on the RPL protocol of the IoT," *Sensors*, vol. 21, no. 9, pp. 1–24, 2021.

ASMA JAHANGEER received the B.S. degree from Bahria University, Islamabad, Pakistan, and the M.S. degree from the Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), in 2022. Her research interests include the IoT security, data encryption and privacy, cloud computing, and machine learning algorithms. She was awarded with fully funded scholarship during her B.S. degree.

SIBGHAT ULLAH BAZAI received the bachelor's and master's degrees in computer engineering from the Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), Quetta, Pakistan, and the Ph.D. degree in information technology (cyber security) from Massey University, Auckland, New Zealand, in 2020. He is currently an Assistant Professor with the Department of Computer Engineering, BUITEMS. His research interests include applying cyber security to disease identification using deep learning, automating exams using natural language processing, and designing local language sentiment corpora and smart city planning. He was a recipient of the HEC HRDI-UESTP Faculty Ph.D. Scholarship. He is a guest editor and reviewer of several journal's special issues in MDPI, Hindawi, CMC, Plosone, and Frontier.

SAAD ASLAM received the Ph.D. degree in electrical and electronic engineering from Massey University, New Zealand. He is currently a Senior Lecturer with the School of Engineering and Technology, Sunway University, Malaysia. He has over 12 years of experience in academia blended with industry exposure. His current research interests include exploiting machine learning for optimizing wireless networks, D2D communication, clustering algorithms, distributed systems, and game theory optimization.

SHAH MARJAN received the B.S. and M.S. degrees (Hons.) from the Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), and the Ph.D. degree from the School of Electronics and Information Engineering, Beihang University, Beijing, China, in 2020. He is currently the Chairperson with the Department of Software Engineering, BUITEMS. He is also engaged in different research groups of bachelor's and master's. His exposure, experience, and knowledge are aiding the unexposed young blood of Pakistan in general and Balochistan in particular. His research interests include broad and comprises of security, encryption, wireless communication, the Internet of Things, blockchain usage, and machine learning algorithms. He was awarded the M.S. degree (Hons.), which led him to secure a fully funded scholarship for his journey in achieving exposure and Ph.D. degree.

MUHAMMAD ANAS received the B.S. degree from the Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), where he is currently pursuing the M.S. degree. His research interests include the Internet of Things, cloud computing, and cyber security. He was awarded with fully funded scholarship during his B.S. degree.

SAYED HABIBULLAH HASHEMI received the dual B.S. degrees in mathematics and physics from Nangarhar University, in 2009, and the M.S. degree in physics (optics and laser) from Bu-Ali Sina University, Iran, in 2021. He is currently an Assistant Professor with the Department of Physics, Paktia University, Paktia, Afghanistan. His research interests include smart agriculture using IoT and AI-based efficient approaches for metal identification.