CYBERNETICS AND PHYSICS, VOL. 12, NO. 3, 2023, 182–193

ROUTING ALGORITHMS IN INTERNET OF THINGS COMPLEX NETWORK WITH THE ROLE OF MACHINE LEARNING

Firuz Kamalov
artment of Electrical Engineering,
Canadian University Dubai,
bai 144534, United Arab Emirates
firuz@cud.ac.ae

Zahra Sayari
Faulty of Engineering,
Deylaman Institute of Higher
Education, Lahijan, Guilan, Iran
Sayyari.s@yahoo.com

Mehdi Gheisari
[1]Young Researchers Club, Parand Branch,
Islamic Azad University, Parand, Iran.
[2]Department of Cognitive Computing,
Institute of Computer Science and Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical
and Technical Sciences, Chennai, India.
mehdi.gheisari61@gmail.com

Cheng-Chi Lee
[1]Department of Library and Information Science,
Research and Development for physical education,
health and information technology,
Fu Jen Catholic University,
New Taipei City 24205, Taiwan
[2]Department of Computer Science
and Information engineering, Asia University, Taiwan
cclee@blue.lins.fju.edu.tw

Sherif Moussa
Department of Electrical Engineering
Canadian University Dubai,
Dubai 144534, United Arab Emirates
smoussa@cud.ac.ae

Article history:
Received 21.04.2023, Accepted 16.09.2023

Abstract

In recent years, the growth of internet-based technologies increased at a rapid pace. The development of technologies such as the Internet of Things (IoT) influenced the enormous increase in the use of data and internet services. IoT devices use different algorithms for facilitating connectivity between devices and control them. However, ensuring smooth connectivity using protocols across a shared medium of network resources is challenging. IoT ecosystems utilize several routing algorithms to deliver the best path/ route for network traffic to control cyber physical systems. These routing algorithms allow IoT networks to use network routes, thereby increasing network traffic mobility effectively. So, a comprehensive survey is needed, which paves the path for researchers. Specifically, this survey investigates and compares the routing solutions in the IoT environment from different perspectives than current surveys such as safety, flow control of data and other essential parameters in IoT physical and nonphysical systems.

Key words

Routing Techniques; D2D; Communication; Internet; IoT.

1 Introduction

The last decade witnessed a rapid increase in the use of smart devices and IoT networks. Kevin Ashton first introduced the concept of IoT cyber physical system in (Ashton, 1999). In the presented research, he envisaged an IoT network similar to the cybernetics. He argued that it would change the world in the same way the Internet did in the late 90s and that IoT does not reduce the time and execution of calculations nor increases communication latency. It aims to provide an intelligent and mechanized environment to meet human's daily needs by combining various active Internet-based technologies in which contextaware computational services facilitate a dynamic communication platform (Razzaque *et al.*, 2016; Singh *et al.*, 2014). In recent years, IoT concepts have been incorporated into the industry for improved data analytics, better communication, and minimal human intervention.

Routing algorithms are considered one of the most influential factors in meeting IoT-based Quality of Service

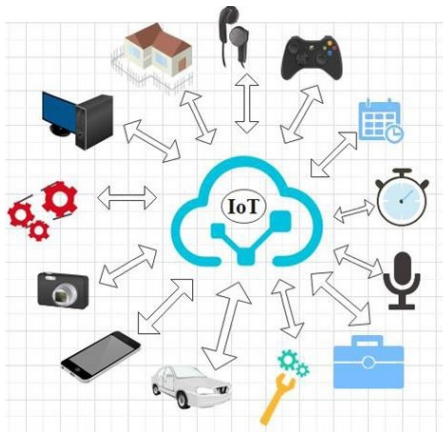

Figure 1. How Internet of Things work.

requirements (Chelloug and El-Zawawy, 2017). In order to communication-related challenges and communication evolution over time, previously-defined routing algorithms do not meet the IoT infrastructure requirements. In detail, IoT devices in medical care, surgery, and driverless vehicles require high-precision, faster, reliable, and error-free algorithms (Dhumane *et al.*, 2016*b*). Due to the fact that selection of efficient routes is one of the most important steps in networks, usually in networks most of the independent routes are considered, while there are many dependent routes that can be more efficient than the main routes, when the network load increases (Melnikov and Terentyeva, 2022). Choosing the suitable routing method helps economically by reducing maintenance costs, development costs or even deployment periods. For example, some routing algorithms are automatically updated at regular intervals, and others are routed according to the user's needs and requests (Razzaque *et al.*, 2016). The suitable routing algorithms are often sensitive to breakdowns and loss of routes. In such scenarios, they quickly provide alternative routes. In the case of a bottleneck, the network traffic in IoT systems is halted, which leads to performance degradation (Weiser *et al.*, 1999). Moreover, they are suffering security and privacy-preservation challenges (Dhumane *et al.*, 2016*b*). Therefore, choosing the suitable routing algorithm in the right scenarios is critical for IoT infrastructures with huge data traffic volumes.

Researchers define the goal of IoT as a socially-aware technology (Singh *et al.*, 2014). Research is underway to ensure that IoT devices are efficient while they are intelligent devices with communication capabilities which can improve the interaction between humans and the environment. When connected to the Internet, such complicated networks might lead to more complications, such as routing challenges, data interaction models challenges, connectivity challenges, and data and cyber security ones. A comprehensive system needs to cater to these challenges in the most efficient possible way (Dhumane *et al.*, 2016*b*). Mark Weiser (Weiser *et al.*, 1999) defines the intelligent environment as a physical world tied highly and invisible with sensors, displays, and computing elements. They are joined in our everyday lives and connected with a continuous network; therefore, the IoT network infrastructure is horizontal (Sharma and Ramkumar, 2019) in nature, where every connected node has the same level of priority, and the data is often processed with traversal or priority strategy. IoT-based communication involves communication models such as the Device-to-Device (D2D) and Machine-to-Human (M2H). However, a significant part of IoT connectivity is based on D2D communication. In this way, it can exchange information among heterogeneous current studies of routing algorithms. The rest of the paper is organized as follows: Sec. 2 presents an overview of IoT and the communication processes. In Sec. 3, routing issues in IoT infrastructure are discussed. Section 4 focuses on current studies of routing algorithms. Section 8 draws the conclusion and suggests future work of this study.

2 Internet of Things (IoT)

IoT is a well-known word. However, its definition changed over time. The main purpose of IoT is to consider the connectivity of smart physical and non-physical devices with the least human intervention. In general, IoT refers to the precise and intelligent connectivity of objects to quickly and efficiently meet the desired needs in a generally smart system. With the increase in the number of smart devices, connections are becoming coherent and harsh to control. For example, today, they use smart ambulances for emergencies or devices across heterogeneous networks in a closed communication environment (Afergan, 2006).

2.1 IoT Applications

IoT applications include a wide range of devices with different scenarios and prerequisites (Poorter *et al.*, 2011). Most of these implications are used in our daily life:

- **Traffic organization:** In IoT, road traffic is managed by intelligent traffic lights, and there is no need to set specific policies.
- **Driverless vehicles:** There is no need for a driver anymore; embedded sensors automatically keep vehicles in line.
- **Earthquake notification:** IoT sensors can detect natural events before they occur.
- **Connected healthcare:** IoT facilities also detect diseases and monitor patients' condition and their remote examination (Singh *et al.*, 2014; Poorter *et al.*, 2011).
- **Smart food containers:** IoT in these containers reduces food waste using RFID technology (Don *et al.*, 2018).
- **Evaluation of global humidity, smoke, and temperature with Techniques of IoT Cloud Computing:** It uses the IoT nodes and protocols to collect

Table 1. Factors Affecting the Communication Process (Dhumane *et al.*, 2016*b*)

Same or different types of nodes in terms of resource	Devices
Different companies, different technologies, policies, algorithms, etc.	Producer and manufacturer
Similar and/ or different networks as source and destination me	Network
Connectivity between two devices (fixed or temporary)	Connectivity
Insufficient and/ or different amounts of resources	Resources
Resource-constrained devices with less or no participation in routing	Participation in messages broad-casting
Variable communication mode (Single-hop or multi-hop)	Communication process
Mobile nodes and dynamic infra-structure	Network topology
Communication diversity among devices of different vendors	Communication
Environmental factors (Rain, high temperatures, etc.)	Environmental conditions
Device addressing scheme	Addressing mechanisms

related data and sends it to the central server for evaluation with high-level security (Jo *et al.*, 2020).

- **Mood Evaluation Tool:** It is an IoT tool for recognizing students' emotional states. It creates an environment appropriate to individuals' emotional states. The tool's purpose is to raise the level of quality of education and learning (Makhija and Wadhwa, 2019).
- **Automotive industry:** IoT uses advanced sensors to satisfy customer needs. On the other hand, by using RFID technology, higher levels of work accuracy can be reached.
- **Retail and Marketing:** IoT's benefits can also be used by retail and marketing, such as knowing the product's invoice or inventory.
- **Transportation:** Deleting paper tickets and collecting tickets electronically on buses and trains is an important aspect of IoT technology.
- **Agriculture and Livestock:** IoT-based agriculture and livestock technologies are being developed at a rapid scale. These areas aim to cater to farmers' and livestock's sophisticated needs in an organized way (Poorter *et al.*, 2011).

3 Background about Routing in IoT

As mentioned previously, IoTs significantly improved citizens' quality of life. In daily activities, smart devices and physical intelligent systems with help users in easing their lifestyles. In terms of technology, innovation, and IoT infrastructure generates a huge amount of data. This data needs to be organized so that the data traffic bottlenecks can be avoided. The recent advances in IoT demonstrate a need to create an intelligent environment where IoT-based big data creation, storage, ownership, cybersecurity, expiration, and routing techniques are well-defined (Tian and Hou, 2010).

Proper routing is critical in IoT infrastructure. In particular, low-power radio links, multihop network topology, battery nodes, and dynamic network topology are all power-hungry techniques (Tawalbeh *et al.*, 2020; Trnka and Cerny, 2016). Due to the various devices and tools covered by the IoT, there is a huge list of challenges in preparing and selecting routing protocols. Since there is an excellent variety of IoT analytics tools, developing a single protocol to achieve all the fundamentally different goals is challenging, as presented in Tab. 1.

3.1 Factors Affecting the Routing Algorithms

In Tab. 1, various factors affecting routing in the IoT are presented.

3.2 Evaluation metrics of Routing algorithms

- Energy-Efficient Routing: Choosing the best and shortest path which reduces energy consumption and increases the network lifetime. By doing so, it intelligently sends information to the destination through the nodes with high energy sources and prevents the nodes with less energy than a specific threshold value from taking part in traffic routing operations.
- The amount of data redundancy: The data produced by IoT devices is redundant. The energy consumption for data routing can be managed by eliminating data redundancy and data integration.
- The amount of delay: In IoT infrastructure, several devices generate and transmit data simultaneously. Therefore, reducing latency plays a vital role in all simultaneously running operations. A reduced communication delay will help deliver the information to the receivers quickly. Consequently, it is necessary to minimize the delay (Dhumane *et al.*, 2016*b*).

3.3 Content Awareness in Routing

Identifying the Five Ws (i.e., Who, What, Where, When, and Why) that are needed for understanding the context and content of a routing scenario has been discussed in (Li *et al.*, 2014). Raw information should be collected from IoT devices and processed by associating

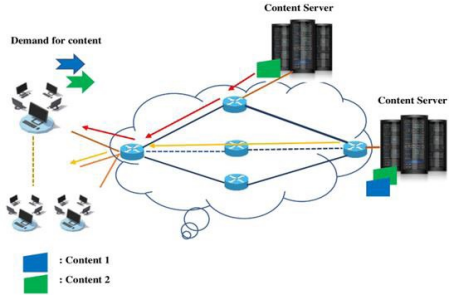

Figure 2. A kind of Content Awareness Routing.

them with their features. These values describe particular attributes. Then, Service quality levels are considered after identifying and pre-processing the service content and context awareness. Therefore, quality assessment of overall system performance depends on cumulative resource utilization since the content varies according to the environment and service. So, we need to be ensured that the available content is concise and valid. This helps in accurate navigation. The next step is to prepare the content for publication in the neighboring nodes.

To do it efficiently, two possible ways can be performed: (1) the content is stored centrally on a server or (2) use a distributed mechanism for content distribution across the network. Both methods have their advantages and disadvantages. Due to the limited energy of nodes and the energy-intensive nature of channel-based communication, the second method is often considered effective. Technical challenges of routing solutions are discussed below:

- Content acquisition and distribution: Due to intelligent routing, raw data must be collected, processed, validated, and converted to a particular content-related format before transmission.
- Content quality: Quality of Context (QoC) should be obtained which is based on parameters such as validity, accuracy, and updates. In QoC, the state depends on factors such as the quality of the sensors, content, and internode communication frequency.
- Text storage: Due to the limited energy, data is often stored within the device. Similarly, due to the limited memory, we need to improve data storage concepts within devices or create a centralized server for the entire network content. Smart routing has several advantages. It includes finding the best route, network load balancing, increasing network lifetime, reducing power consumption, secure routing and reducing latency.

4 Current Studies of Routing Algorithms in IoT

In this section, state-of-the-art developments in IoT routing protocols are presented. The advantages and disadvantages of these developments are also high-lighted.

4.1 Ad-hoc Routing Protocol of Multipath Distance Vector-based on Demand for IoT

The solution covers all types of IoT devices, including connected nodes and connection-less nodes (Prasad and Sharma, 2022). Each device keeps internet-connected information in one table and its routing information in another. The destination IP is considered an Internet linking address (ILA) when the device connects to the Internet. Then, the Internet Connecting Table (ICT) value is calculated. In the next step, it is ensured that ICT has a node that is appropriate for connecting to the Internet. If ICT has such a node, the ILA address will be replaced by the destination node's IP address. Otherwise, a Route Re-quest Message (RREQ) is sent to examine the routing and ICT table contents.

Also, this protocol is required to find the route on request.

The four main messages used by this protocol during the process include:

- RREQ: Used to search for a route to the destination
- RREP: Respond to the source RREQ message (such as the ACK message) and send the RREP destination.
- RERR: To inform other neighboring nodes of the nodes with which they were connected and are now out of reach
- HELLO: Protects routing tables from periodic intervals.

The authors evaluated and compared their solution based on several metrics which have been explained deeply in (Tian and Hou, 2010).

4.2 MRP Secure Multi-Hop Routing Protocol

This protocol is focused on increasing security by preventing malicious attacks [19]. At first, each IoT network owner must register their details, such as services, network addresses, and data-link addresses, and a suitable provider (SP). SP creates an Encrypted File (EF), installing it on any personal device before establishing a network based on the information provided (Dhumane *et al.*, 2016*b*).

Also, HELLO messages will be broadcasted on the network after a specific time interval. This message's header which is received from device number one, is compared with the other device's HELLO message's header. Two different devices can communicate when they send a HELLO message simultaneously. After connecting a device X to an IoT network, it will send a communication request to device Y. Checking the URL of the device X data link in the EF file will start with the network address of device Y. Upon joining the IoT network, if the service running on it matches with the service running on the device Y, a signal is sent for generating HELLO message in an encrypted form. A timer synchronizes all IoT devices with a predetermined amount. Simultaneously, the scrambler module changes the order of "reserved" bits for improved security.

4.3 Routing Protocol over Low Power and Lossy Networks

The LoWPAN6 networks have low power and weak radio communications, power supply nodes, multi-hop network topologies, and frequent topological. The International Engineering Task Force (IETF) presented a new protocol suitable for low-power and weak networks (Iova *et al.*, 2015). It has been contemplated as a standard routing for IoT, which attempts to develop the routing for convergent traffic patterns. It is also a distance-vector protocol, which commences from a border router, and creates a non-circular Destination-oriented Guideance Graph (DODAG) by using one or more criteria.

DODAG is created to improve the link costs, device attributes, and objective functions in which the objective function performs IoT device ranking. It also supports multiple traffic types, including multi-point-to-point, point-to-multipoint, and point-to-point traffic. For a loop-free topology, ranks are increased from the roots to the leaves uniformly. It supports a unique ranking for complex networks. According to the content of each application, low links are split into several different parts. Multiple non-consistent DODAGs with independent roots can also be created. Various RPLs can run simultaneously on devices, and RPL Instance ID is used for unique sample identification. Network topologies are performed by the DODAG Information Option (DIO) messages. These links are regularly broadcasted and linked to the root of the creation and maintenance of DIO route messages. These messages contain important information like the DODAG identifier, objective function, node rank, or metrics. After receiving the DIO message, the neighboring nodes adjust their rank based on the neighbor's rank. A special message is used to retrieve routing information from leaf nodes of the roots and is often termed a DODAG wave expansion process (Iova *et al.*, 2015). Several related works have been proposed on top of it since it has shown its great performance.

4.4 Multipath Routing in RPL

This routing protocol aims to increase the net-work lifetime by protecting more limited energy nodes to consume less energy. In this algorithm, the network lifetime is considered before any node's death due to the energy completion bottlenecks. The authors proposed an Expected Lifetime (ELT) metric to indicate the node's remaining time in (Perera *et al.*, 2013). They created DODAG, which depends on the ELT metric to indicate the life-time of all routes to the border routers accurately, and designed a mechanism to identify the bottlenecks for extending the traffic load to several parents. They made other contributions to allocating traffic load to each router and distributing energy consumption fairly across all routes to the border routers. As a result, only a part of the traffic reaches a particular bottleneck, and the energy consumption is well-balanced (Perera *et al.*, 2013).

4.5 PAIR (Pruned Adaptive IoT routing)

IoT helps intermediate nodes get monetary profit by providing a pricing model since different stakeholders own it. They often use their own resources for transferring data. The following parameters are used for each relay node using the PAIR protocol:

- Residual energy and energy consumption
- Current load and buffer space
- Distance to the neighbor

PAIR works in two steps: The first step is called the forward step. In this step, startup messages are sent to neighbors. These messages contain the cost from the source to the current node. Intermediate nodes broadcast these messages to their neighbors after updating the cost. An acknowledgment from the destination nodes is received for selecting the best route. The second step is called the regressive step. If the ack message fails, it sends a routing message to the neighbor node to avoid failure. An active path be-tween source and destination is created, and data transfer is initiated. It is a multi-path and content-aware routing protocol. It solves the issues of collaboration among heterogeneous network nodes by adding some incentives for relay nodes. The nodes use a large amount of energy to transmit data. An attempt to lighten the communication for easy data transmission creates challenges such as data security and high data usage.

4.6 Energy and Link quality Routing Protocol (REL)

The REL protocol uses the wireless link and residual energy quality during the route selection process to increase system reliability and QoS for different IoT applications. Low-power radio and noise sensitivity, interference, and multiple interferences can distort a wireless communication link. One of the most reliable indexes using the REL while analyzing a link is the Link Quality Index (LQI). REL, stores N possible routes to the destination. It selects them based on the following criteria: The first one is to check the quality of wireless links based on the low links criteria. Then, it measures the residual energy and considers the number of steps for avoiding lengthy and inefficient routes (Dhumane *et al.*, 2016*a*).

The route selection process depends on two factors: Firstly, the number of thresholds HDdiff max - the energy threshold, and secondly, allowed ETH. The energy threshold is used to choose the route and load balancing mechanism using the load balancing optimization mode. If E represents the energy levels' inclusion, then the computational difference between current E (t) and the previously recorded energy level E (t-1) provides information about the new remaining energy. This helps the neighboring nodes to re-evaluate the use of a node in their routes if the difference is significant and higher than E. Otherwise, if the value of E is low, it represents

uniform energy consumption. Higher values show relatively large differences in the energy utilization of nodes.

4.7 Optimal QoS-aware multi-path routing (OQM)

OQM considers IoT devices' lifespan and density levels to find the best route. In this way, it uses a specific criterion to estimate the cost of each node. It also stores the reachable node information in a unique table to select the best neighbor group. In the next phase, the primary nodes spread the particular request (also known as route discovery request) to find the node's right path. The best node is decided based on the cost level, lifespan, and density level. It may be noted that selected nodes are checked for lifespan and density level at particular time intervals (Ahmed *et al.*, 2020*a*). The authors evaluated it from several perspectives and found it optimal QoS rather than current studies.

4.8 Smart Collaborative Routing protocol (SCR)

SCR is a secure, high-speed tree-based protocol. In this protocol, after identifying parents' and children's devices, each device can only pass the packets to the parent and its child's devices. If two nodes are close to each other but with different parents, the packet takes a long way to arrive at the destination as Figure 3 shows.

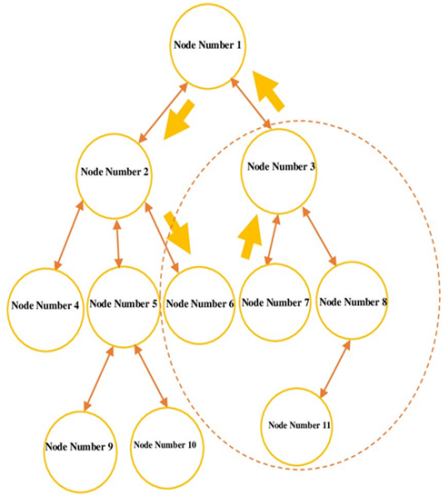

Figure 3. Forwarding Packets

To address the challenge effectively, the authors added the neighbor rule. In this rule, each device has its next hope node information. Adding this rule helps in transmitting the packet directly. If a problem causes a parent or child node to be disconnected, the tree structure continues to work with existing nodes and topology updates. Another benefit of this routing protocol is multi-casting packets to find the nearest route, thereby saving energy, cost, and time (Zhu *et al.*, 2020).

5 Security Challenge in Routing

Having mentioned the routing challenge and current studies in this regard above, they are suffering from security and privacy challenges which are one of the most important issues in IoT's routing algorithms. By enhancing these two factors, people and companies can trust this infrastructure more and more. The threat can be stealing important data or exchanging them with fake data. Particularly, the attacks can be applied to the network under the following groups (Zhu *et al.*, 2020):

1. Devices with the operating system (such as IOS, Android, ...)
2. Attack the webcams, surveillance cameras, and the IoT devices such as smart homes, and sniff their information and data
3. The crimes that illicit activities are often in great public demand
4. The crimes related to traffic monitoring and public places such as railways, etc
5. Attacks on devices with wireless connection and in a physical layer such as Bluetooth

Technically, famous attacks are (Ahmed *et al.*, 2020*b*):

Sybil attack
Bad-Mouthing
Ballot Stuffing
On-Off attack
Opportunistic Services
Black-hole, Grey-hole, and Worm-Hole
Crude/Self Recommendation

The IoT framework still needs more expansion, but there are many obstacles to development, such as the application domains and individual security levels for each user and device. Because of the fact that the security in IoT is very sensitive for each client, many organizations are focused on it by facing new challenges and finding new solutions for them. Figure 4 shows the IoT's network architecture and layer which may be affected by attackers and adversaries (Dongre *et al.*, 2022).

Each layer includes its own specific threats; for example, domain-related threats are applied in the application layer, while the threats related to the end devices and IoT devices can be in the perception layer the most important worries about IoT's security are respectively distinguishing, entrance, verification, authorization, and trust across all modules, devices, and components in the IoT framework. In the following, some of the most important approaches to deal with these threats are described:

5.1 Generic IoT Layers and Data Fusion Framework

This framework proposed by the authors in (Tawalbeh *et al.*, 2020) is based on the cloud and consists of the cloud, IoT devices, and clients (end users). In this model, the present entities of the device layer include WSDs (Wireless Sensors Devices), which can collect data, transmission protocols, and devices that send data

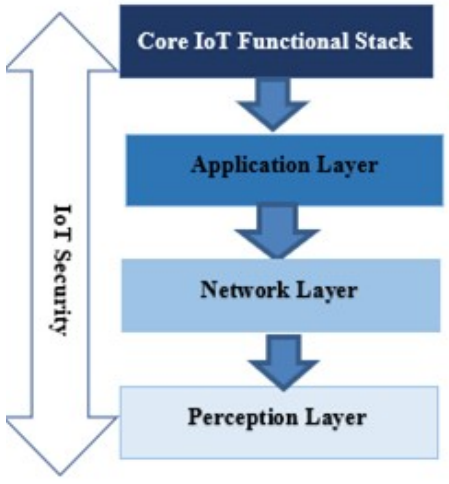

Figure 4. IoT's Network Architecture

to the depository. The cloud layer is where the data are gathered for feature processes like noise canceling and future derivation. The authors' approach is applied before the implements are added to the secure network. The parts of this model are software and hardware, transmission model. Figure 5 is a summary of this framework.

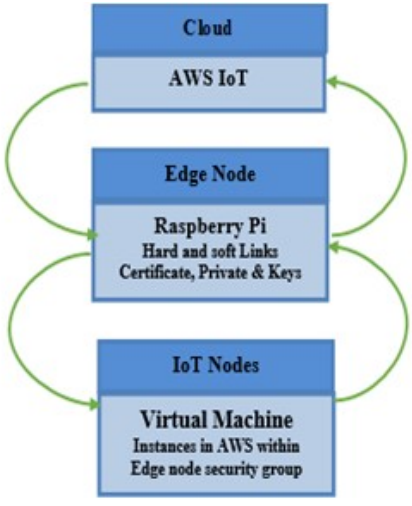

Figure 5. Summary of Generic IoT Layers and Data Fusion Framework

Also, the main feature of this model is the implementation of secure protocols and cryptography between each layer (Tawalbeh *et al.*, 2020).

5.2 CID Framework (Central Identity Framework)

This is a security framework that stores all device records. It assigns an individual identifier to each device that connects to the network as bear-up Role-Based Access Control. All devices in the network should authenticate among these rules. This authentication process can build trust between devices forging a more effective secure routing algorithm. Figure 6 shows a diagram of this framework (Trnka and Cerny, 2016).

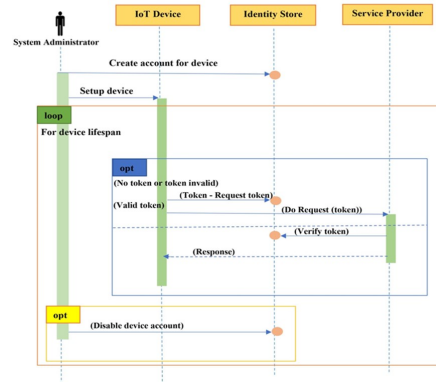

Figure 6. Diagram of CID framework

Each device needs a token in this framework to communicate in the network. This token is allocated from the identity store. Note that having a dedicated account with specific rules for each available device is necessary. This framework supports both authentication and authorization. The authorization is supported by OAuth 2 protocol and JWT token. All-round monitoring and administrator powers in this framework in-crease security so that at any moment, the administrator is able to maintain security.

5.3 HFSDT-IoT (Hybrid Framework for Securing Data Transmission)

This framework is designed to enhance the security of IoT infrastructure and its components, such as secure routing, which can detect and prevent the net-work from Dos-Security threats. To meet these goals, this framework consists of two phases. In the first phase, a customized Ethereum PoS protocol is running. Ethereum PoS is formed on an intelligent contract that can be specialized for each application and device. Also, the intelligent contracts are updated with both the attack list and the protected one. Due to the fact that this framework is based on a blockchain mechanism, In the second phase, to increase safety, communications are using cross-blockchain and secp256k1 encryption (Kharrufa *et al.*, 2017). Figure 7 depicts the framework from an abstract point of view.

5.4 IoT Framework Based on SDN and NFV (Software-defined Networking and Network Function Virtualization):

To have a stable network with high-level security, the authors bring a framework with both SDN and NFV

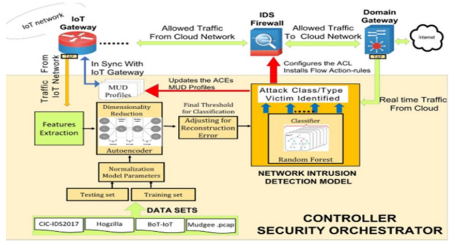

Figure 9. IoT Framework Based on SDN and NFV

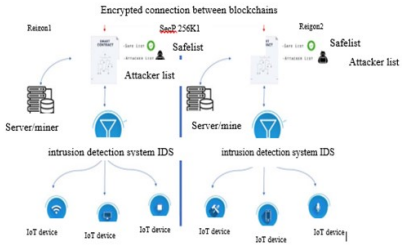

Figure 7. The diagram of HFSDT-IoT framework

technologies. In this framework, NFV is responsible for providing security dynamically, whereas SDN routes network traffic. The four layers that make up the network in this framework include the Device, Connectivity, Network Control, and Intelligence Layer. The device layer includes all devices in the network, such as sensors, end devices, and so on. NFV, in this part, implements and supports the security of devices and applications. In the connectivity layer, SDN switches route traffic to the special destination in the upper layer if necessary. The network control layer handles the network traffic and provides the services' security. The last layer, the Intelligence Layer, contains the blocks for security actions, information, context data, traffic information, and so on. The rules and security devices are also in this layer (Ong and Peradilla, 2021). Figure 8 is the diagram of this framework.

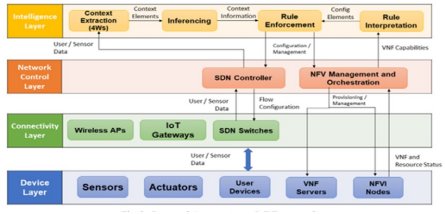

Figure 8. IoT Framework Based on SDN and NFV

5.5 MUD-Based Behavioral Profiling Security Framework

This security framework contains smart security and multiple IDSs that scan/defend MUD-compatible IoT/multi-access edges in the network. This framework strongly acts against edge network attacks by scanning the network. Note that MUD consists of standards and goals of IoT devices that connect to the network. Also, the MUD-Based Behavioral Profiling Security Framework introduces a new mechanism for detecting anomaly (Krishnan *et al.*, 2022). Figure 9 is the Security controller architecture of this framework.

6 Machine learning and Deep Learning in IoT applications

Machine learning and deep learning can help to improve not only the security level of the network but also the better classification of the enormous data privacy and load balancing of the network traffic (Kamalov *et al.*, 2020). Moreover, algorithms which are based on machine learning and deep learning can cover all the different types of network communication and applications in the IoT network. In the following, some of the most important machine and deep learning applications in IoT infrastructure have been described.

6.1 PEARL(Power and Delay-Aware Learning-based Routing)

This routing algorithm is based on machine learning that uses routing rules and Objective Function (OF) to find the best route with the slightest delay and using less power. It should be noted that OF use the Q-learning approach and one hopes E2E (End-to-End) delays to find the best route. Also, in PEARL, the selected links, their routing information, and their capacity are controlled by DIO messages. To implement the routing rules, PEARL uses parent devices which in each area receive DIO messages (Lalani *et al.*, 2022).

6.2 DBSCAN-R (Density-Based Spatial Clustering)

This solution is formed based on DBSCAN (density-based spatial clustering for applications with noise). The most important feature of DBSCAN is data clustering without setting the number of clusters. Instead of giving the cluster number, it clusters by the density of the neighbor nodes and the number of devices in each area. Authors did not limit themselves and leveraged DBSCAN-R; in DBSCAN-R, the effective in-formation will be extracted. This information consists of the number of devices used as the middle nodes to get the data and send to the destination IoT device, the free and utilized space of the buffer of a device, the distance between the corresponding device and the relay, which is usually calculated by the Euclidean distance and the number of successful delivered packets of each node (Pillai *et al.*, 2022). DBSCAN-R flowchart is shown in Fig. 10 .

6.3 Energy-aware Routing Algorithm

This algorithm is divided into four parts. In the first part, after the division of the network, In each area, a node with the same cover area is slept by fuzzy-chaotic

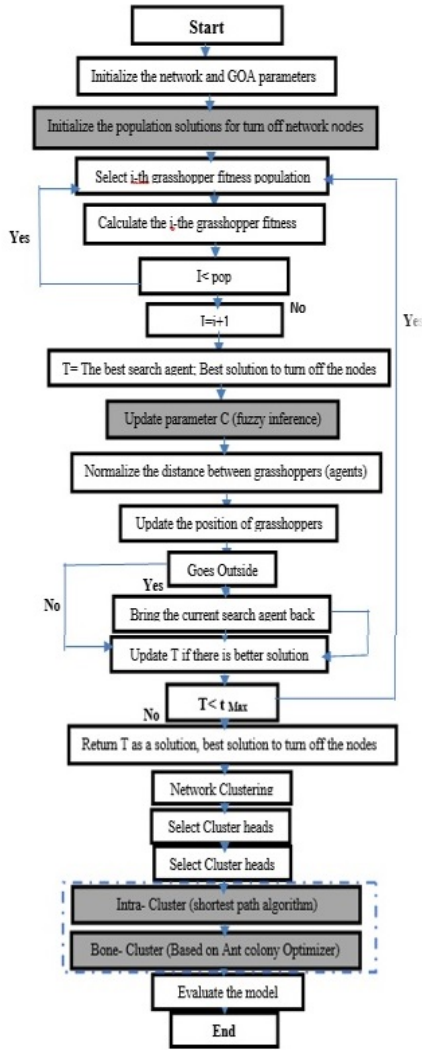

Figure 11. Energy-aware Routing Algorithm

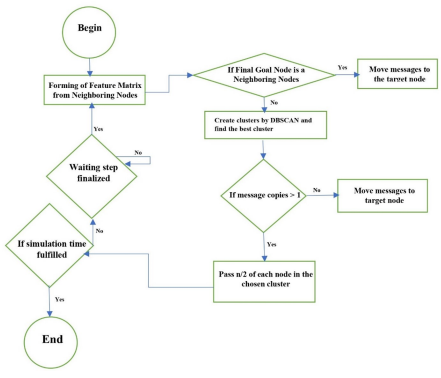

Figure 10. Flowchart of DBSCAN-R

grasshopper algorithm. After the first part, the cluster head is selected in each area by the periodic method. Finally, the routing is done by selecting the nearest and best paths in two phases. The first phase is about sending the packet to the cluster head, and then the process of sending the packet to the destination area is started (second phase). Fig 11 has depicted the routing algorithm (Mir *et al.*, 2022).

6.4 DLIRS(Deep Learning based Intelligent Routing)

This routing algorithm uses deep learning (DL) to find the best route in the network. It has two phases. The first phase is about setting Convolutional Neural Network (CNN) for each path combination. In the first phase, the other routing algorithm is used to learn the CNNs then the trained CNNs will be used in the second phase. In the second phase, the trained CNNs will be retrained, data will be gathered, and the pathes will be refreshed (Zabeehullah *et al.*, 2022).

7 Future Research Challenges

Data routing in a heterogeneous network is a real challenge. The success factor of routing mechanisms depends upon different parameters. Although there is a primary classification, the routing in IoTs is at an early stage. There are various obstacles that researchers still face. A few of them are discussed below:

7.1 Content awareness

In IoT, devices play the role of agents. By collecting the environment's contents and analyzing them to create required intelligent routing information, agents are used to making routing decisions. Available protocols are mainly used for the residual energy of the nodes. Apart from residual energy, which is often referred to as the main parameter other essential parameters such as node memory, processing power, and link quality often require improvement (Frey *et al.*, 2014).

7.2 Shortage of plan to evaluate the trust of the network

Due to there is a lot of ways to communicate between nodes and devices, such as p2p and several kinds of networks in the IoT, there are no unique schemes to evaluate the trust in this humongous network (Ahmed *et al.*, 2020*a*).

7.3 Key management

Symmetric key management scheme is a fundamental challenge for cryptography and big data access in IoT (Mohamed, 2021).

7.4 Radio band

For communication or data transfer, each device needs its own dedicated bandwidth; with the increasing number of devices under the Internet of Things, the need for dedicated bandwidth is getting more attention (Frey *et al.*, 2014).

7.5 Data security

Data security and privacy-related authentication is often required before connecting two devices. This helps in preventing data theft. These scrutiny techniques are

vital because data is routed through different networks with different owners. Moreover, to ensure that the routing algorithms do not violate individuals' privacy laws, security policies must consider as crucial points. Therefore, algorithms must support encryption and security solutions to protect users' privacy, security, and confidentiality (Gheisari *et al.*, 2019; Mollah *et al.*, 2017; HaddadPajouh *et al.*, 2021; Pazmino *et al.*, 2019; Kamalov *et al.*, 2020; Kamalov *et al.*, 2023*a*; Kamalov *et al.*, 2023*b*).

7.6 Congestion

Often referred to as bottleneck, the congestion-related constraints lead to an expiration of IoT-generated data. Therefore, it should be ensured that the data should be transmitted to the destination within the desired time frame (Dhumane and Prasad, 2017).

7.7 Lack of expertise

The digitalization of the IoT infrastructure often requires the care and maintenance of equipment. A detailed study on the care and expertise list is presented in (Pazmino *et al.*, 2019).

7.8 Deaths of nodes

Excessive and unnecessary energy usage might lead to node expiry. Unfortunately, it is not possible to replace dead-nodes batteries. Similarly, due to the high density, the physical replacement of these nodes is also a hectic task. To face these challenges, energy holes are created to halt, divert, and manage the routing processes.

7.9 Scalability

Many IoT devices use wireless and wired communication mediums. These devices are either fixed or mobile. Mobile devices may enter or leave the network randomly, thereby increasing or decreasing the network size and routing capability (Hajjar *et al.*, 2017; Gheisari *et al.*, 2023; Moshayedi *et al.*, 2023; Moshayedi *et al.*, 2022)

7.10 Change of topology

Due to various reasons, the network topology changes. One of the best solutions is to provide a reactive or hybrid routing protocol that can easily administer these network changes (Raj and Basar, 2019).

7.11 Heterogeneity

IoT infrastructures use various technologies. The term "heterogeneity" means a network's ability to allow many technologies, devices, and standards to incorporate. However, this highly increases network complexity. In recent years, the need for routing protocols for supporting heterogeneity has been increasing (Whitmore *et al.*, 2014).

7.12 Multi-path Routing

Multiple routing techniques are used to perform load-balancing operations. This helps in increasing network productivity. Setting up a network with too many routing features is also harmful, as network resources can be easily misused. Therefore, the network topology's soft-reconfiguration means fewer control packets with fewer control packets and lower energy consumption. This ultimately extends network lifetime. Besides load balancing, multi-path routing is also used to improve tolerance of errors, reliability, and QoS performance.

8 Conclusion and Future Works

The Internet has changed over the last decade. It is due to the advancement of sensor technology and easy access to cheap hardware. Today, sensor-based connectivity is simpler and cheaper than ever before. Similarly, due to the advent of IPv6, the nomenclature and addressing scheme for network devices is easier. As a result, data routing techniques witnessed an enormous increase. This paper discussed the existing routing algorithms, including those that are secure and leverage Machine Learning based on several metrics. Also, it examined the importance of content awareness and incentive-based relaying mechanisms in the routing process. It discussed the factors affecting the routing process at different stages, such as nodes, point-to-point, and two-way routing. Finally, the challenges and future research are posed that can help other researchers in the future. As one future work, we plan to evaluate the solutions on the basis of more metrics, such as privacy-preserving degrees.

References

Afergan, M. (2006). Using repeated games to design incentive-based routing systems. In: *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*. pp. 1–13.

Ahmed, KI, M Tahir and SL Lau (2020*a*). Trust management for iot security: Taxonomy and future research directions. In: *IEEE Conference on Application, Information and Network Security (AINS)*.

Ahmed, KI, M Tahir and SL Lau (2020*b*). Trust management for iot security: Taxonomy and future research directions. In: *IEEE Conference on Application, Information and Network Security (AINS)*. pp. 123–134.

Ashton, Kevin (1999). *That 'Internet of Things' Thing*. Scientific Research Publishing.

Chelloug, Samia Allaoua and Mohamed A El-Zawawy (2017). Middleware for internet of things: Survey and challenges. *Intelligent Automation & Soft Computing* pp. 1–9.

Dhumane, A., R. Prasad and J. Prasad (2016*a*). Routing issues in the internet of things: A survey. In: *Lect. Notes Eng. Comput. Sci. Proc. Int. MultiConference Eng. Comput. Sci*. Vol. 1. pp. 404–412.

Dhumane, Amol V. and Rajesh S. Prasad (2017). Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT. *Wireless Networks* **25**(1), 399–413.

Dhumane, Amol V., Rajesh S. Prasad and J. Rajendra Prasad (2016*b*). Routing issues in internet of things: A survey. In: *Proc. Int. MultiConference Eng. Comput. Sci*. Vol. 1 of *Lect. Notes Eng. Comput. Sci.*. pp. 404–412.

Don, Venura S. A. Abeysinghe Achchige, Seng Wai Loke and Arkady B. Zaslavsky (2018). Iot-aided charity: An excess food redistribution framework. In: *Proc. 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*. pp. 1–6.

Dongre, N., M. Atique, Z.A. Shaik and A.D. Raut (2022). A survey on security issues and secure frameworks in internet of things (iot). In: *IEEE International Conference on Smart Systems and Inventive Technology (ICSSIT)*.

Frey, Michael, Friedrich Grose and Mesut Gunes (2014). Energy-aware ant routing in wireless multi-hop networks. In: *2014 IEEE International Conference on Communications (ICC)*. IEEE.

Gheisari, Mehdi, Fereshteh Ebrahimzadeh, Mohamadtaghi Rahimi, Mahdieh Moazzamigodarzi, Yang Liu, Pijush Kanti Dutta Pramanik, Mohammad Ali Heravi, Abolfazl Mehbodniya, Mustafa Ghaderzadeh, Mohammad Reza Feylizadeh and Saeed Kosari (2023). Deep learning: Applications, architectures, models, tools, and frameworks: A comprehensive survey. *CAAI Transactions on Intelligence Technology* **8**(3), 581–606.

Gheisari, Mehdi, Quoc-Viet Pham, Mamoun Alazab, Xiaobo Zhang, Christian Fernandez-Campusano and Gautam Srivastava (2019). ECA: An edge computing architecture for privacy-preserving in IoT-based smart city. *IEEE Access* **7**, 155779–155786.

HaddadPajouh, Hamed, Ali Dehghantanha, Reza M. Parizi, Mohammed Aledhari and Hadis Karimipour (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things* **14**, 100129.

Hajjar, Ayman El, George Roussos and Maura Paterson (2017). Secure routing in IoT networks with SISLOF. In: *2017 Global Internet of Things Summit (GIoTS)*. IEEE.

Iova, Oana, Fabrice Theoleyre and Thomas Noel (2015). Using multiparent routing in RPL to increase the stability and the lifetime of the network. *Ad Hoc Networks* **29**, 45–62.

Jo, JunHo, ByungWan Jo, JungHoon Kim, SungJun Kim and WoonYong Han (2020). Development of an IoT-based indoor air quality monitoring platform. *Journal of Sensors* **2020**, 1–14.

Kamalov, F., S. Moussa, R. Zgheib and O. Mashaal (2020). Feature selection for intrusion detection systems. In: *2020 13th international symposium on computational in-telligence and design (ISCID)*. IEEE. IEEE. pp. 265–269.

Kamalov, Firuz, Behrouz Pourghebleh, Mehdi Gheisari, Yang Liu and Sherif Moussa (2023*a*). Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. *Sustainability* **15**(4), 3317.

Kamalov, Firuz, Mehdi Gheisari, Yang Liu, Mohammad Reza Feylizadeh and Sherif Moussa (2023*b*). Critical controlling for the network security and privacy based on blockchain technology: A fuzzy DEMATEL approach. *Sustainability* **15**(13), 10068.

Kharrufa, Harith, Hayder Al-Kashoash, Yaarob Al-Nidawi, Maria Quezada Mosquera and A.H. Kemp (2017). Dynamic RPL for multi-hop routing in IoT applications. In: *2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. IEEE.

Krishnan, P., M. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal and H. Song (2022). Mud-based behavioral profiling security framework for software-defined iot networks. *IEEE Internet Of Things Journal* **9**(9), 6648–6660.

Lalani, S.L., B. Safaei, A.M. Monazzah and A. Ejlali (2022). Pearl: Power and delay-aware learning-based routing policy for iot applications. In: *2022 CPSSI 4th Interna-tional Symposium on Real-Time and Embedded Systems and Technologies (RTEST)*. IEEE.

Li, Shancang, Li Da Xu and Shanshan Zhao (2014). The internet of things: a survey. *Information Systems Frontiers* **17**(2), 243–259.

Makhija, Shikhar and Bimlesh Wadhwa (2019). Mood board: An IoT based group mood evaluation tool. In: *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE.

Melnikov, B. and Y. Terentyeva (2022). An approach for obtaining estimation of stability of large communication network taking into account its dependent paths. *Cybernetics and Physics* **11**(3), 145–150.

Mir, Masoomeh, Mahdi Yaghoobi and Maryam Khairabadi (2022). A new approach to energy-aware routing in the internet of things using improved grasshopper metaheuristic algorithm with chaos theory and fuzzy logic. *Multimedia Tools and Applications* **82**(4), 5133–5159.

Mohamed, Mona (2021). A comparative study on internet of things (iot): Frameworks, tools, applications and future directions. *Journal of Intelligent Systems and Internet of Things*.

Mollah, Muhammad Baqer, Md. Abul Kalam Azad and Athanasios Vasilakos (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications* **84**, 38–54.

Moshayedi, Ata Jahangir, Atanu Shuvam Roy, Alireza Taravet, Liefa Liao, Jianqing Wu and Mehdi Gheis-

ari (2023). A secure traffic police remote sensing approach via a deep learning-based low-altitude vehicle speed detector through UAVs in smart cites: Algorithm, implementation and evaluation. *Future Transportation* **3**(1), 189–209.

Moshayedi, Ata Jahangir, Jinsong Li, Nima Sina, Xi Chen, Liefa Liao, Mehdi Gheisari and Xiaoyun Xie (2022). Simulation and validation of optimized PID controller in AGV (automated guided vehicles) model using PSO and BAS algorithms. *Computational Intelligence and Neuroscience* **2022**, 1–22.

Ong, A.V. and M. Peradilla (2021). An iot framework based on sdn and nfv for context-aware security. In: *International Conference on Ubiquitous and Future Networks (ICUFN)*.

Pazmino, Leandro, Fanny Flores, Luis Ponce, Juan Zaldumbide, Viviana Parraga, Byron Loarte, Gabriela Cevallos, Ivonne Maldonado and Richard Rivera (2019). Challenges and opportunities of IoT deployment in ecuador. In: *2019 International Conference on Information Systems and Software Technologies (ICI2ST)*. IEEE.

Perera, Charith, Arkady B. Zaslavsky, Peter Christen and Dimitrios Georgakopoulos (2013). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials* **16**, 414–454.

Pillai, Rohan, Rashmi Rao, Challa Rahul Prasad, Apoorva Rao Iragavarapu and Annapurna D (2022). DBSCAN-r: A machine learning approach for routing in opportunistic networks. In: *2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. IEEE.

Poorter, De, I. E., Moerman and P. Demeester (2011). Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented architecture. *J Wireless Com Network*.

Prasad, Sanjeev Kumar and Tripti Sharma (2022). Performance comparison of multipath routing protocols for mobile ad hoc network. *International Journal of Systems, Control and Communications* **13**(1), 82–98.

Raj, Jennifer S. and Abul Basar (2019). QOS OPTIMIZATION OF ENERGY EFFICIENT ROUTING IN IOT WIRELESS SENSOR NETWORKS. *Journal of ISMAC* **01**(01), 12–23.

Razzaque, Mohammad Abdur, Marija Milojevic-Jevric, Andrei Palade and Siobh?n Clarke (2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal* **3**(1), 70–95.

Sharma, Ishu and K.R. Ramkumar (2019). Analysis of manet payload delivery behaviour with parallel routingthrough mimo. In: *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. pp. 1–4.

Singh, Dhananjay, Gaurav Tripathi and Antonio J. Jara (2014). A survey of internet-of-things: Future vision, architecture, challenges and services. *2014 IEEE World Forum on Internet of Things (WF-IoT)* pp. 287–292.

Tawalbeh, L., F. Muheidat, M. Tawalbeh and M. Quwaider (2020). Iot privacy and security: Challenges and solutions. *MDPI Journal, Appl.* **10**(12), 4102.

Tian, Yicong and Rui Hou (2010). An improved AOMDV routing protocol for internet of things. In: *2010 International Conference on Computational Intelligence and Software Engineering*. IEEE.

Trnka, M. and T. Cerny (2016). Identity management of devices in internet of things environment. In: *International Conference on IT Convergence and Security (ICITCS)*. IEEE.

Weiser, Mark D., Rich Gold and John Seely Brown (1999). The origins of ubiquitous computing research at parc in the late 1980s. *IBM Syst. J.* **38**, 693–696.

Whitmore, Andrew, Anurag Agarwal and Li Da Xu (2014). The internet of things—a survey of topics and trends. *Information Systems Frontiers* **17**(2), 261–274.

Zabeehullah, Fahim Arif and Yawar Abbas (2022). DLIRS: Deep learning based intelligent routing in software defined IoT. In: *2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. IEEE.

Zhu, M., L. Chang, N. Wang and I. You (2020). A smart col-laborative routing protocol for delaysensitive applications in industrial iot. *IEEE Access*.