International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209699 Volume 8, Issue 4, July – August (2021)

SURVEY ARTICLE

A Survey on Issues and Possible Solutions of Cross-Layer Design in Internet of Things

Sultana Parween
Department of Computer Science, Jamia Millia Islamia, New Delhi, India.
sultana.tech@gmail.com

Syed Zeeshan Hussain
Department of Computer Science, Jamia Millia Islamia, New Delhi, India.
szhussain@jmi.ac.in

Md Asdaque Hussain
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
asdaque@kluniversity.in

Received: 07 June 2021 / Revised: 08 July 2021 / Accepted: 14 July 2021 / Published: 28 August 2021

Abstract – Last decade has seen the evolution of Internet of Things (IoT) and it has been affiliated with various networking technologies. The study shows that blending various networks like WSN, WBAN, and LoRaWAN with digital devices will revolutionize the current decade. Billions of wireless devices will cooperate and communicate with each other to generate huge data every day. The heterogeneity of devices and communication network technologies are inherent in IoT. Various digital devices are connected and interact with various devices, which have different specifications and run on different platforms. Therefore, the heterogeneity of network architecture, communication technologies, and application requirement intricacy enforce many challenges. Traditional communication technologies which rely heavily on layered approach need an amendment to suit the need of the IoT as various layers (e.g. Transport layer's TCP) fails to address the issues of heterogeneity. This work reviews various cross-layer mechanisms extensively, which have been suggested in past to overcome the issue and challenges which arose due to the heterogeneous nature of IoT. We also identify the main issues such as energy consumption, mobility, interoperability, security, privacy, and scalability, etc. faced when using cross-layer design (CLD) in IoT and suggest available cross-layer solutions for them.

Index Terms – Internet of Things (IoT), Cross-Layer Design (CLD), Wireless Sensor Network (WSN), Quality of Service (QoS), Low Power Wide Area Networks (LPWAN), Privacy, Security, Energy-Efficient, Interoperability.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have included a wide range of wired or wireless connected devices that are commonly used in monitoring the environment and collecting data. As per Cisco, the number of connected devices will be above 500 billion at the end of 2030. An intelligently handling system for such a huge range of communicating devices as well as all the collected data is a new thing that belongs to IoT. WSNs specific devices can sense, process, and store information and then transmit it to a data center over the entire network. The WSN terminology was implemented almost 30 years ago and was initially suggested for military surveillance. This technology was then applied in many other fields, such as climate, environment, agriculture, and surveillance of wildlife successfully.

More effort was needed before WSNs could dynamically enhance our everyday lives. On the other hand, IoT applications may extend from smart kitchens to smart cities. WSN is responsible for network safety whereas IoT helps people to quickly access and exchange information easily anytime and anywhere [1]. Wireless communication technology contributes significantly to the expansion of IoT technology. WSN will also change the look and behavior of various applications and industries.

The tiny, robust, affordable and low-powered WSN sensors will bring the IoT to even the smallest objects mounted in any type of environment, at a fair cost [2]. So, wireless sensor networks and IoT would impact positively the qualitative living in the world. In fact, WSN is the most important element in IoT paradigm. Various issues emerge while integrating the WSN and IoT under cross-layer design. These issues include performance problems, mobility, privacy and scalability, energy efficiency, interoperability, and security.

SURVEY ARTICLE

1.1. The Motivation of This Article

Constant advances and ever-increasing demands from current terminology tend to inspire scientists and researchers to create new standards. In comparison, there has been significant growth in the various related terminology i.e. Big data, cloud computing, WSN, IoT, etc., in the nascent years. Thus, bearing in mind the present scenario of continuous developments in the area of IoT, there was a critical need to research the actual functions and capacities of modern age IoT concepts. This paper highlights the basic principle of IoT and the need for cross-layer architecture in IoT. It recognizes the main issues faced by IoT and their possible solutions.

1.2. This Survey Paper is Organized as Follows

- Overview of IoT paradigm, its evolution, the taxonomy of architecture, application, and various communication technologies. (Section 2).
- Cross-layer architecture for WSN and IoT (Section 3).
- Potential issues and their possible solutions (Section 4).
- Conclusion (Section 5).

Figure 1 shows a pictorial representation of the organizational structure for the paper.

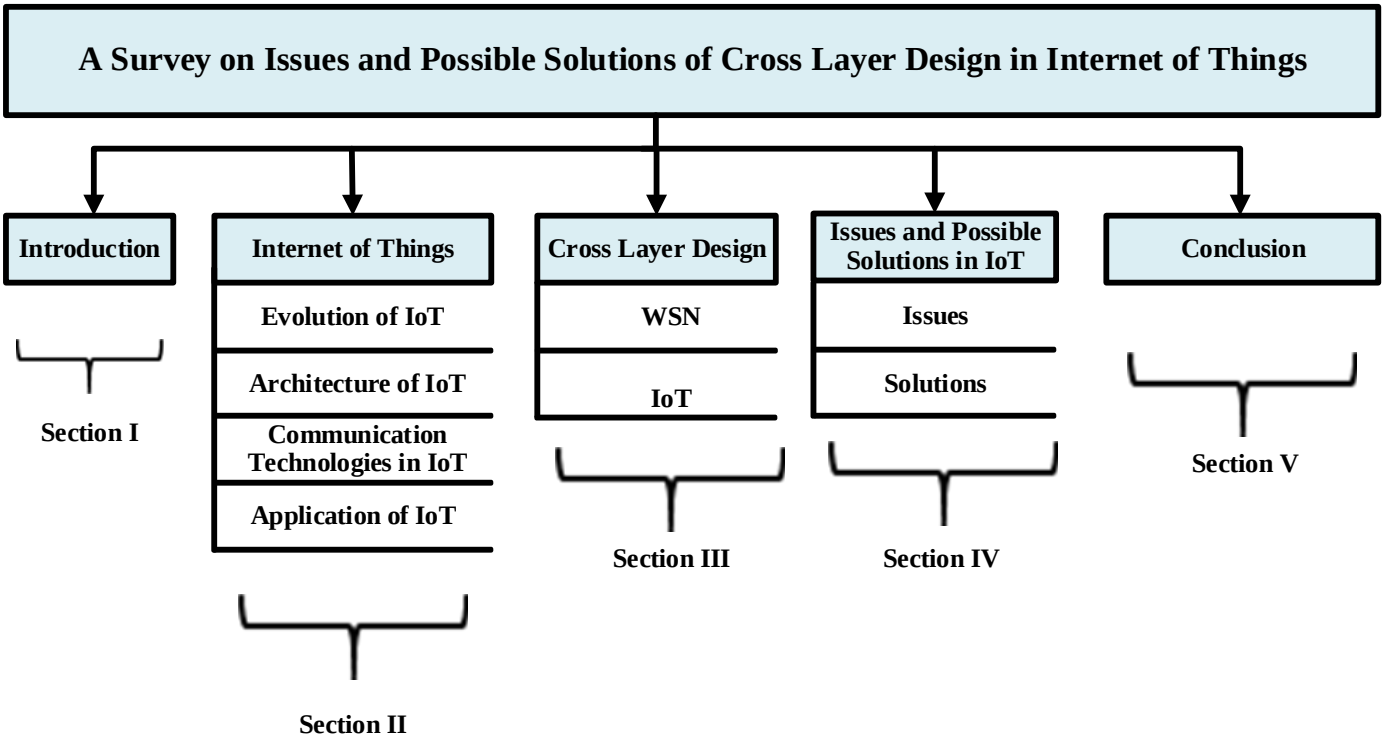

Figure 1 The Organizational Structure of the Paper

2. IOT: AN OVERVIEW

2.1. Evolution of the IoT

IoT is a novel technology, increasing rapidly in the modern wireless telecommunications scenario [3]. The IoT can be viewed as things that are interconnected with the network, whereas things are linked wirelessly by smart sensors. IoT is capable to communicate without human intervention [4]. IoT is a network of objects integrated with RFID chips and related technologies so that the objects could connect and interact with each other [5]. Thus, it is also possible to connect different physical devices with the assistance of IoT. There are several benefits of IoT but with the increased number of devices used within IoT, more problems arise towards wireless communication among the devices. Due to which there is a rapid increase in the quality of services involved.

In the early 1990s, Kevin Ashton first introduced the most important buzzword "Internet of Things" at the Massachusetts Institute of Technology (MIT) Auto-ID Laboratories [6]. The term IoT was coined using RFID-enabled devices for detection and tracking. RFID and sensors are integrated into IoT that allows the development of industrial services along with the expansion of service deployment in new applications [3]. Since 2010, IoT has been able to network a wider range of "things" with improvements in the area of smart sensors, sensor network technologies, and low-energy wireless networking. IoT included a range of recent technologies like cloud computing, WSN, smart sensing, low-energy wireless communications, NFC, mobile computing, etc. that allow an

SURVEY ARTICLE

IoT to configure networks, sensor networks, and eventually ubiquitous networks [7]. IoT trend is the fusion of sensing and the internet; where all networked objects must be flexible, smart, and sufficiently autonomous to deliver the services required. It would offer the communication and incorporation needed into our everyday lives. The evolution of the Internet of Things can be shown through many stages in Figure 2.

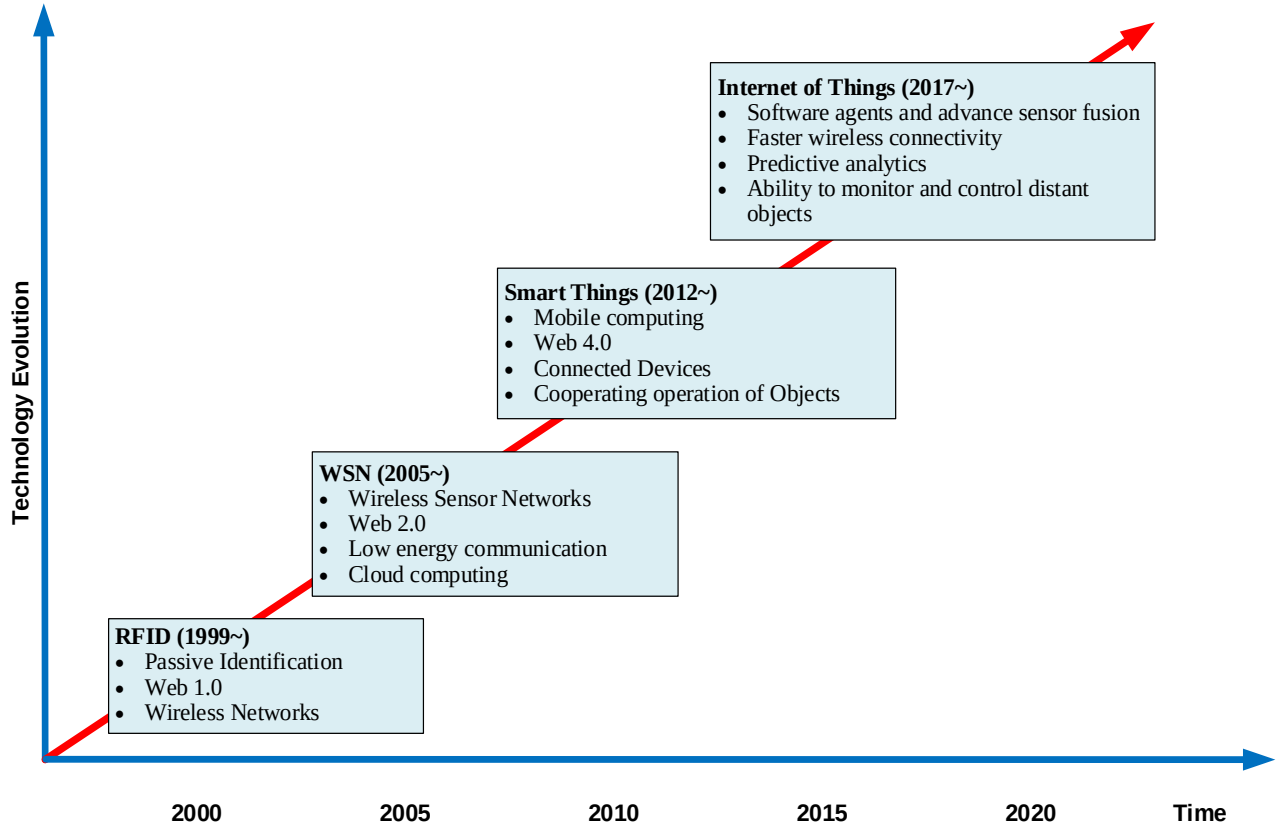

Figure 2 Evolution of IoT [4]

2.2. Architecture of IoT

The IoT architecture is suggested by many researchers but there is no particular architecture that all the researchers support. The generally known architectures are the three-layer architecture and the five-layer architecture. The three-layer architecture is the simple structure that was presented in the initial investigation phases. The five-layer architecture has been developed later when the three-layer architecture was not able to satisfy the requirements of applications and many issues were faced in security and privacy regarding IoT.

2.2.1. Three-layer Architecture

The development of IoT principle is based primarily on its design. IoT has basically three layers at the initial stages of the study: the perception layer, the network layer, and the application layer [8]. Figure 3 depicts the three-layered architecture and described in the following subsections.

2.2.1.1. Perception Layer

This layer is also called the "Physical Layer" or "Sensing layer". It acquires data from the physical environment with the aid of sensors and actuators [9].

2.2.1.2. Network Layer

The main function of this layer is the transmitting and routing of data gathered from various IoT sensors to different IoT devices and transferred across the Internet. It uses various communication technologies to control various network devices, such as routers, switches, and gateways.

2.2.1.3. Application Layer

It is the topmost layer in the 3-layer architecture that provides actual services to the customers. It is accountable for confidentiality, authenticity, and data integrity. The objective of IoT is accomplished at this layer [10].

SURVEY ARTICLE

2.2.2. Four-layer Architecture

The four-layer architecture was created to comply with all IoT requirements. It has three layers similar to three-layer architecture, but it also has an extra layer known as the "Support layer". Figure 4 illustrates the four-layer architecture of IoT.

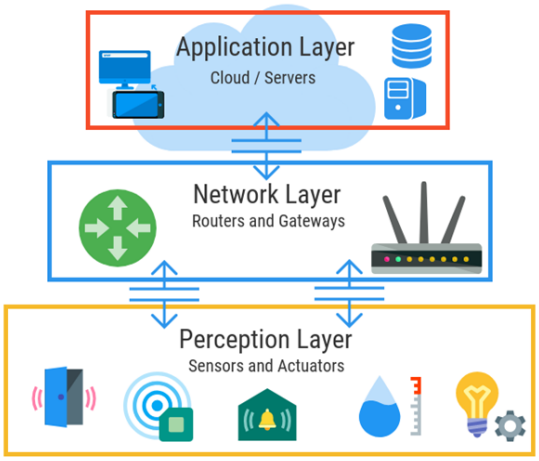

Figure 3 Three-Layer Architecture [11]

2.2.2.1. Support Layer

The primary reason for implementing the support layer is to make a secure IoT architecture. There were several security flaws in the three-layer architecture when the information is transmitted directly to the network layer. The data from the perception layer is sent to the support layer [12]. It has two primary functions: It ensures the data is safe from attacks and is transmitted by authentic users and then transmits the data to the network layer. It utilizes the authentication method to verify the user.

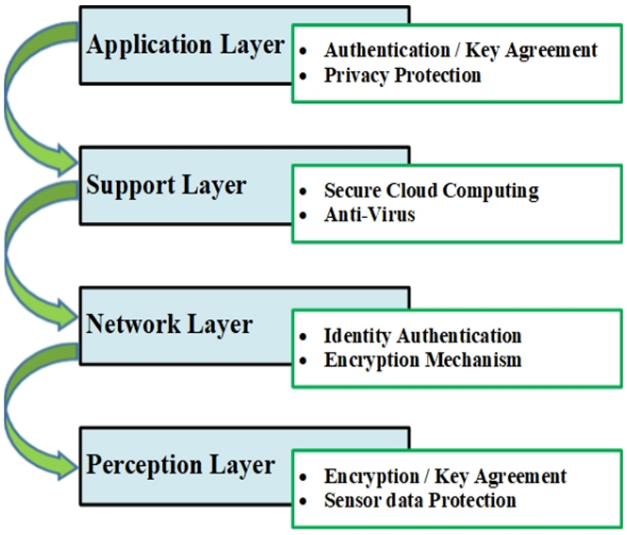

Figure 4 Four-Layer Architecture [13]

2.2.3. Five-Layer Architecture

This architecture plays a significant role in IoT development by addressing the security and storage problems in four-layer architecture. It has three layers similar to the three-layer architecture and also includes Middleware and Business layers as shown in Figure 5.

2.2.3.1. Perception Layer

This layer operates in the same manner as mentioned earlier in the three-layer architecture [14]. This is used for taking information from the sensors and implementing them.

2.2.3.2. Network Layer

Sometimes the Network layer is named as "Transmission layer". This layer takes data from the Perception layer and is transferred to the Middleware layer [15].

2.2.3.3. Middleware Layer

This layer is also named as "Processing layer" in IoT architecture. It analyses, stores, and processes the huge amounts of data that come from the Network Layer.

2.2.3.4. Application Layer

This layer is responsible for inclusive application management based on the processed data in the Middleware layer [16].

2.2.3.5. Business Layer

This layer acts as the manager of the entire system. The main function of this layer is to manage and control applications, business, and profit models [17].

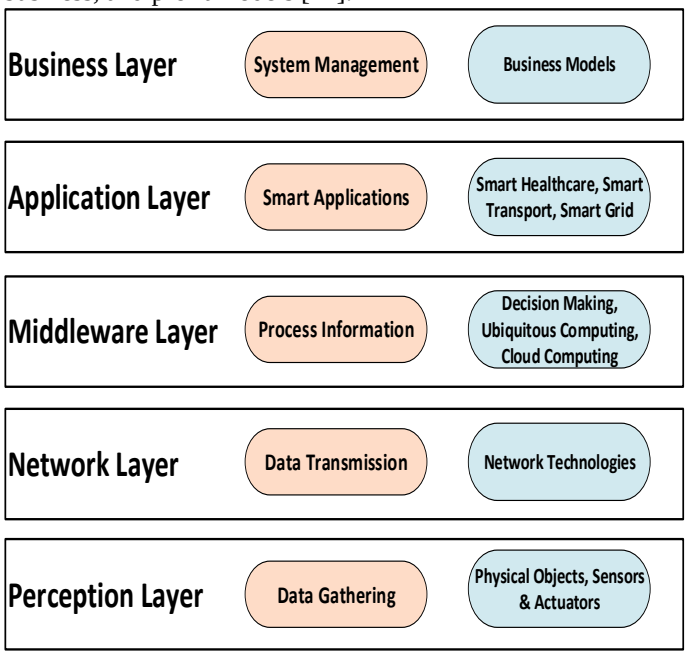

Figure 5 Five-Layer Architecture [12]

SURVEY ARTICLE

2.3. Wireless Communication Technologies for IoT

There are several wireless communication technologies that have been developed today for IoT applications. Each communication technology has its own set of benefits as well as its drawbacks [18]. The following paragraph gives a critical assessment for each wireless communication technology in IoT: -

2.3.1. RFID

IoT concept was developed using RFID technology for automatic identification, authentication, and tracking. It operates in a 433 MHz to 3.11 GHz frequency band. The RFID consists of an RFID reader and tag and antenna. An antenna is used to transfer signals among the tag and reader. Tag systems have two technologies: the first one is known as active RFID and the other is known as passive RFID. Active RFIDs are costly and use higher frequencies and it is associated with the battery. A passive tag transfers ID to the active RFID readers [19].

2.3.2. NFC

Near Field Communication is in some way similar to RFID configuration. It incorporates an RFID reader into a mobile phone that helps to make it faster, reliable, and more efficient for the consumers. NFC is an extremely short-range, low-power wireless technology with a 13.56 MHz frequency band.

2.3.3. Bluetooth

Bluetooth is developed by the Special Interest Community (SIG) of Bluetooth. It is low cost and generally used for short-range communication among devices for data transmission. It uses frequency hopping spread spectrum(FHSS) to avoid co-existence. Generally, the Master-slave approach is followed in Bluetooth networks. BLE is the version of this standard that was introduced to provide low cost and low power consumption. Data rates vary from 1 Mbps to 24 Mbps in different versions. One of the disadvantages is the limitation of only one-to-one contact between two devices at a time [20].

2.3.4. ZigBee

ZigBee is a popular, low-power wireless IEEE 802.15.4 based communication technology. ZigBee offers communication between IoT devices within the range of 10-100m. It consumes less energy and very cost-effective technology.

2.3.5. Z-wave

Z wave has been extensively employed in smart homes and commercial applications. It is composed of two forms of the device (control and slave). Slave node properties are low-cost machines, and cannot initiate messages. This can only answer and execute the command sent through controlling devices that initiate messages inside the network. The data rate varies from 9 to 40 kbps approximately [21].

2.3.6. LoRaWAN

LoRaWAN was recently developed by the LoRaTM Alliance. It defines the LPWAN standard specifically for IoT applications. The data processing rates of 0.3 kbps to 50 kbps. It works within 868 and 900 MHz ISM bands for communication. Node battery life that is connected usually very long, up to 10 years. LoRaWAN also guarantees secure communication with symmetric key cryptography while authenticating end-users with the networks.

2.3.7. Sigfox

SigFox is an LPWAN technology for wireless communication with many low-energy objects. It requires small volumes of data to be carried up to 50 kilometers. It uses carrier signal Ultra Narrow Band (UNB) technology to increase the bandwidth efficiency. The data processing rates vary from 10 to 1,000 bps.

2.3.8. DASH7

DASH7 is an LPWAN protocol that works at two-level narrowband in the 433 MHz ISM band using the GFSK modulation technique. It is based on standard ISO / IEC 18000. It consumes less energy and also assists in extending battery life. It predominantly opts for tree network topology.

2.4. Applications of the IoT

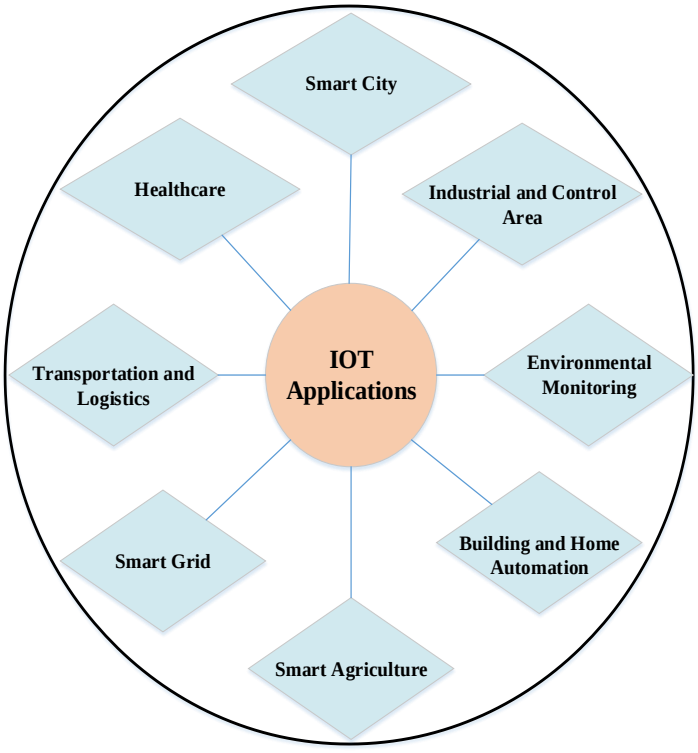

Figure 6 Applications of IoT

SURVEY ARTICLE

There are a variety of domains and environments where these IoT applications can make our lives better. Figure 6 shows the various applications of IoT in the above mentioned areas. The applications of IoT can be divided into the following application areas: -

2.4.1. Healthcare

IoT is used to provide medical services by using wearable sensors like checking heart rate, body temperature, calories, etc. The medical sensors may be wearable, portable, and body-implanted sensors. The Wearable's examples are a fit bit, reflex. Sensors inserted within the body are often of another kind [22]. These are used where continuous monitoring of the health of the patients is needed.

2.4.2. Transportation and Logistics

In the transport and logistics sectors, IoT plays a crucial role. After adding RFID tags or barcodes to the vehicles, the industries can track real-time information of the vehicle, such as vehicle location and others. In addition, one can monitor vehicle speed by improving IoT capabilities in the field of transportation. In logistics, companies can monitor commodity inflow and outflow by making use of barcodes.

2.4.3. Environmental Monitoring

Numerous sensors are available for sensing parameters like humidity, temperature, air, and water pollution. Temperatures are measured using sensors such as RTD and thermometer. We can employ dust sensors and gas sensors to analyze air pollution. The presence of chemicals can be detected by using e-Tongue and e – Nose technologies. Such systems allow the use of pattern recognition software. These are also used to control pollution levels in cities.

2.4.4. Smart Grid

Smart Grid is an electrical grid that is specifically designed for collecting and analyzing data obtained from transmission lines, distribution substations, and applications. IoT can implement technologies in Smart Grid. IoT's comprehensive sensing and processing capabilities can enhance Smart Grid capabilities. Integrating IoT and Smart Grid can significantly promote the implementation of smart nodes, meters and sensors, information equipment, and communication devices.

2.4.5. Smart Agriculture

In this field, IoT is commonly referred to as Smart Farming. Farmers need to use this technology to modernize farming methods, harvesting, weather prediction, water conservation, wildlife management, and so on. It can also detect and control disease spread among animals and plants. The condition of the land can be studied through the use of soil sensors. Farmers can use drones for field monitoring.

2.4.6. Smart City

Smart cities may be defined as a complex IoT paradigm, aimed at managing public affairs through the introduction of ICT solutions. It can make more efficient use of public resources, leading to an improvement in the quality of services provided to the citizen and a significant decrease in public administration operating costs.

3. CROSS-LAYER DESIGN(CLD)

The next sections will describe the CLD methods in WSN and the Internet of Things(IoT).

3.1. Cross-Layer Design in WSN

CLD allows each layer to exchange information between any of the layers in the network model without violating the layered architecture. It may also allow each layer to determine its function and share its information based on information gathered or received by the other layers. In [23] authors have described different cross-layer design approaches in WSN and also have highlighted challenges faced implementing Cross-layer design in WSN.

3.1.1. Categorization of CLD

CLD may be broken down into two main groups based on the sharing method inside a single node: Non-manager and Manager method [24].

3.1.1.1. Non-Manager Method

In this scheme, the pair of layers are allowed to interact with each other in a straightforward way as shown in Figure 7. The architecture of the network model layers cannot be changed. The only modification that takes place is in the protocol functionality of some layers by enabling them to interact among the layers in a straightforward way.

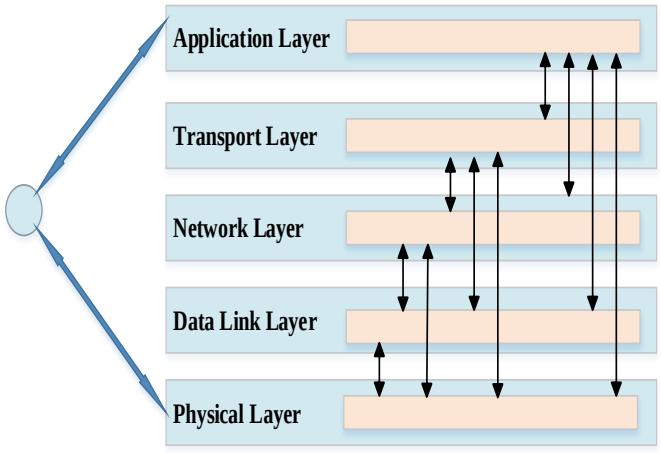

Figure 7 Non-Manager Method [23]

Examples: -

CLD enhances the performance of TCP through CL

SURVEY ARTICLE

interaction among the TCP layer and the bottom layers [25]. So, it is basically a form of non-manager method.

3.1.1.2. Manager Method

In this method, the pair of layers cannot directly interact with each other. The vertical plane works as a manager which is used to exchange information with all layers. The architecture of the network model layers cannot be changed. The only modification that takes place is in the protocol functionality of some layers by enabling them to share information with the vertical plane [26] as shown in Figure 8.

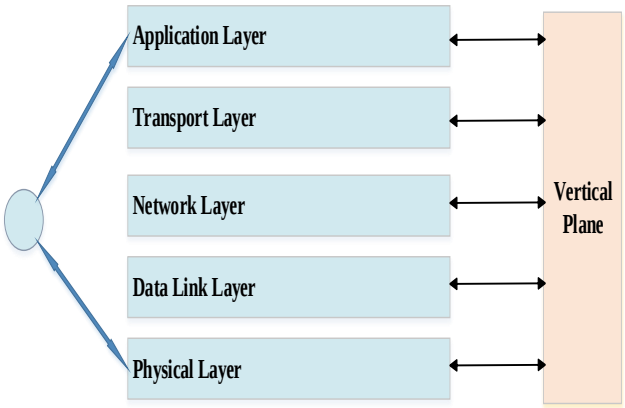

Figure 8 Manager Method [24]

The major difference between the above two methods is that the non-manager method provides straightforward communication among any two layers. But a vertical plane is required for the manager method to provide interaction between two layers. Based on the information sharing method between all the nodes in a network, we can further classify the CLD into two main categories: Centralized method and Distributed method

3.1.1.3. Centralized Method

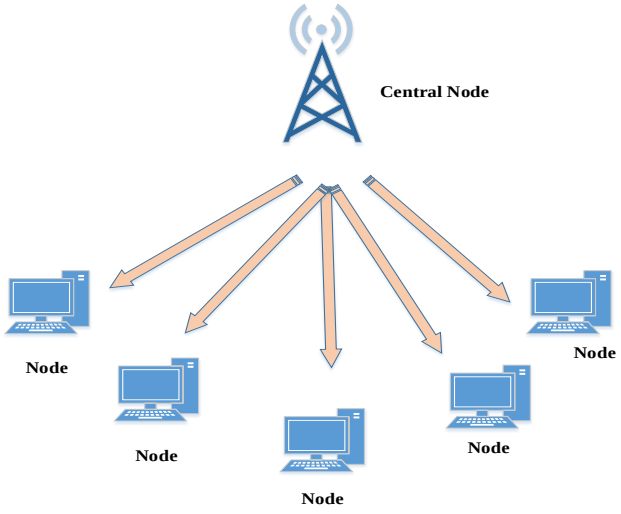

Figure 9 Indicates the Centralized Method [24]

In this approach, a central node is presented in a hierarchical way as shown in Figure 9. It helps to exchange and manage the sharing of information between the two nodes of TCP/IP layers. This approach is generally used in the cellular network.

3.1.1.4. Distributed Method

In this approach, the cross-layer information sharing between nodes by the organization of the network. There is no central node in this method for the sharing and management of information by cross-layer. All the nodes communicate the information with each other directly and handle it separately. Figure 10 shows the distributed method.

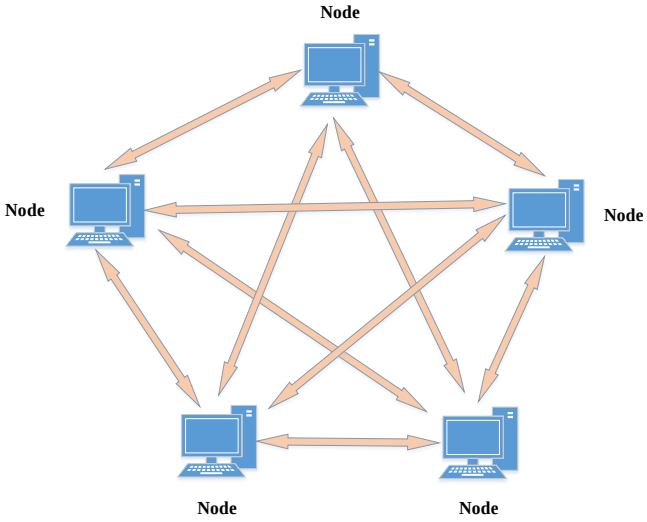

Figure 10 Indicates the Distributed Method [24]

3.2. Cross-Layer Design in IoT

IoT has become a continuously growing concept in ICT that has a wider scope. Due to the most important feature of information hiding in cross-layer architecture that makes it more appropriate for IoT. So, cross-layer communication helps in the field of IoT in several ways. The cross-layer technology is consisting of three layers that contribute a crucial part in improving the performance of IoT platforms. The layers of CLD are the Sensing layer, Network Layer, and Application layer [27]. The Three-layer modular design has several disadvantages due to the feature of data hiding. It allows layers to exchange useful information amongst themselves and leads to redundancies at different levels. So, the performance of the system is also reduced. In comparison, the use of cross-layer architecture allows different protocols that can exchange information according to the requirement at different layers. Thus, certain encryption techniques can be used to enhance security when essential information is transferred to other devices. IoT systems have several devices that are also heterogeneous because each system uses its own concept in such a manner that there's no standardization.

SURVEY ARTICLE

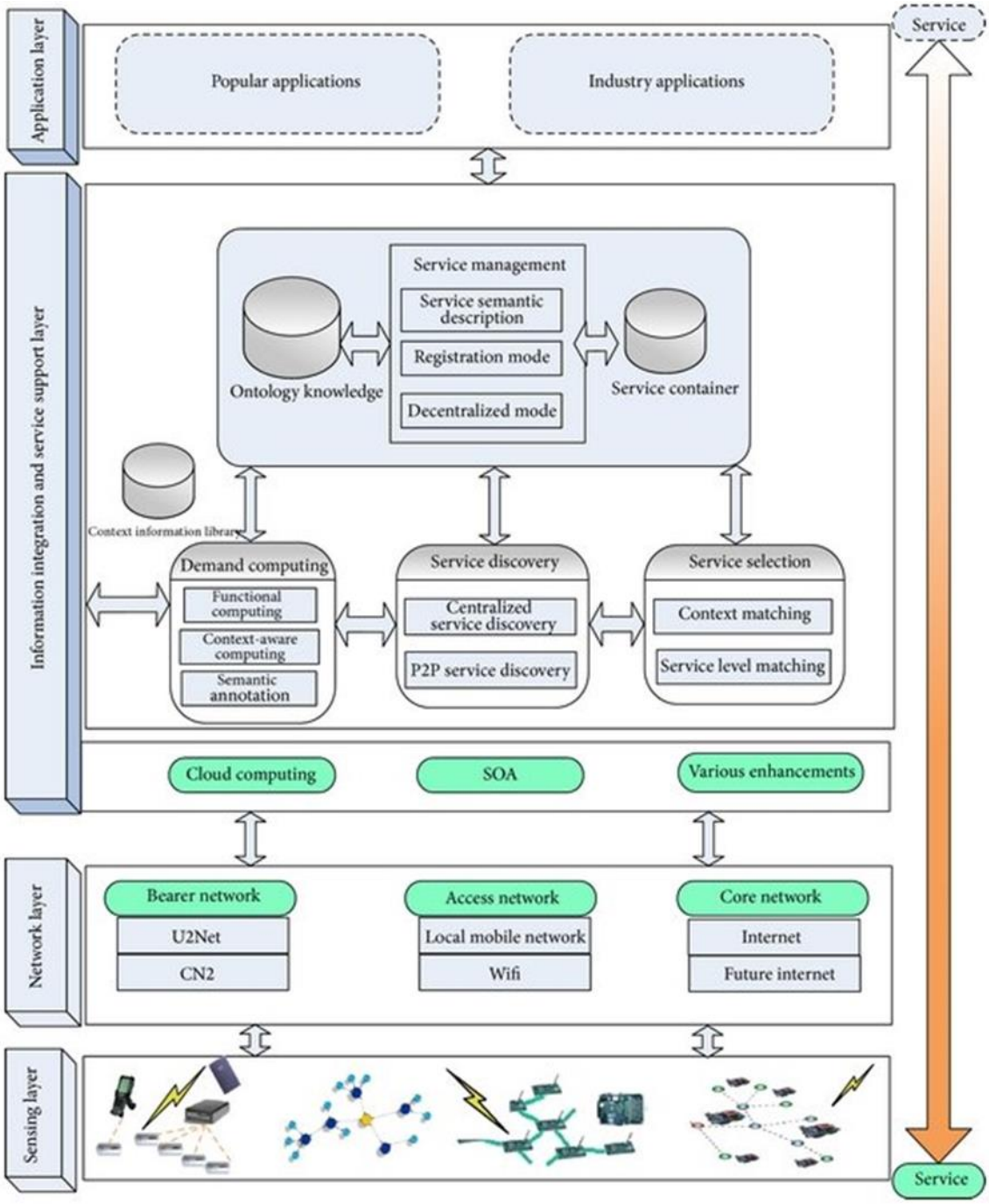

Figure 11 IoT Service Platform Architecture [29]

It leads to security problems whenever data is moved from one system to another system. So, cross-communication aids to provide better levels of protection compared to the simple layered approach. The core objective or problem-solution by this approach is to provide both fluid and intelligent services for numerous IoT users [28]. The service platform of IoT should be extended to ubiquitous service from the conventional common service as its service is expanding to ubiquitous environments such as wireless networks and ubiquitous sensor networks. Thus, to meet this extension of IoT semantic-based cross-layer IoT service platform has been proposed in Figure 11. It is based on the standard of IoT architecture and the semantic-based IoT service framework [29].

SURVEY ARTICLE

This platform includes the four-layer architecture which adds an information integration and service support layer. The Upper layer accomplishes its work by calling in the lower layer service. [30]. The sensing layer aims at achieving real-world sensing. This layer is typically used in the collection of basic data. The Network layer helps in getting the information about service-related network characteristics [31]. The Application layer is responsible to present the particular business service in specific fields, which include popular applications as well as industrial applications. The main components of IoT service platforms are the service support layer and data integration that includes service selection, service discovery, and service management [32].

3.2.1. Service Management Module

This module is accountable for the standardization of service management and description. They used the service registration center model to handle the service registry, upgrade, delete, etc. But for the ubiquitous services, they used dynamic autonomous techniques and obtained decentralized management based on the loosely coupled P2P network. The multiple service registration that is considered as a service node cannot be integrated into a catalogue. So by using the decentralized strategy, a loosely coupled P2P service network is formed among them.

3.2.2. Service Container

This module is capable of loading services. It is specifically for the registration center model based on a semantic UDDI repository that holds all registered service documentation.

3.2.3. Ontology Knowledge

This module contains the ontologies and concepts associated with IoT service platforms.

3.2.4. Service Discovery Module

This module uses various search and matching algorithms and finishes the searching and matching of the service based on the service's management style [33].

3.2.5. Demand Computing Module

This module achieves the user's exact needs through user interaction. It comprises functional computing, context-aware computing, and semantic annotation. Functional requirements are used in understanding what the user needs to do.

3.2.6. Context Information Library

This library is utilized to store the high-level context after fusion as well as the original context information.

3.2.7. Service Selection Modules

This module comprises service level matching and context matching.

4. CRUCIAL ISSUES IN IOT WITH POSSIBLE CROSS-LAYER SOLUTIONS

The cross-layer design of IoT system is used to share information between various layers to achieve complete interoperability between application services and nodes. As a consequence, it creates a potential number of issues and challenges in the system such as security issues, energy consumption, mobility issues, privacy and scalability, adaptability and interoperability between the layer, etc. CLD has its own issues and on integrating this design with IoT, issues are being moved with advantages of the CLD. Some of the problems which faced are being described briefly and further the solutions to these problems are also suggested but these solutions are not the final ones, a better solution can be explored with the passage of time.

4.1. Energy Efficiency Issues

IoT networks consist of low-power devices, but providing energy-efficient devices and sensors is the main challenge for IoT technologies. IoT device performance is determined by power consumption. It is considered to be more efficient if a device uses less power. IoT devices have many benefits and are seen as a growing technology. But it absorbs more energy because of the collective device and sensor communication. IoT framework must incorporate energy efficiency in CLD.

4.1.1. Existing Solutions

In IoT framework, the devices should use less power to provide more efficiency and for that cross-layer approaches might be implemented for energy optimization. In [34], the author introduced a new cross-layer strategy to improve energy efficiency in various IoT applications i.e. ELITE. It reduces the consumption of energy in an IoT node by minimizing the strobe packet transmissions in the RDC protocols of the MAC layer. It makes use of SPR (Strobe per Packet Ratio), a technique designed for usage with asynchronous MAC protocols. It significantly lowers the amount of data sent between source and destination nodes. The Energy Efficiency evaluation results in Figure 12 display that ELITE minimizes the total energy consumption of nodes, when compared to OFFL, DELAYOF, and MRHOF.

They used the On-Line node-level energy calculation technique [35] to estimate the total energy absorbed by each installed motes. The average energy consumption (E_{tot}) is determined by equation 1.

$$E_{tot}=V.[I_c t_c + I_{lopm} t_{lopm} + I_{trm} t_{trm} + I_{rcp} t_{rcp} \sum_{i=1}^{n} I_{per} t_{per}] \quad (1)$$

Where, E_{tot} - the total energy consumed by the nodes.

V - supply voltage of the platform.

I_c- draining current in active mode from the processor.

SURVEY ARTICLE

I_{lopm}- drained current in low power mode.

I_{trm} and I_{rcp}- the drawn currents from the transceiver module in transmission and reception phases.

I_{per}- the current of peripherals.

t- the time spent in a given mode by each module.

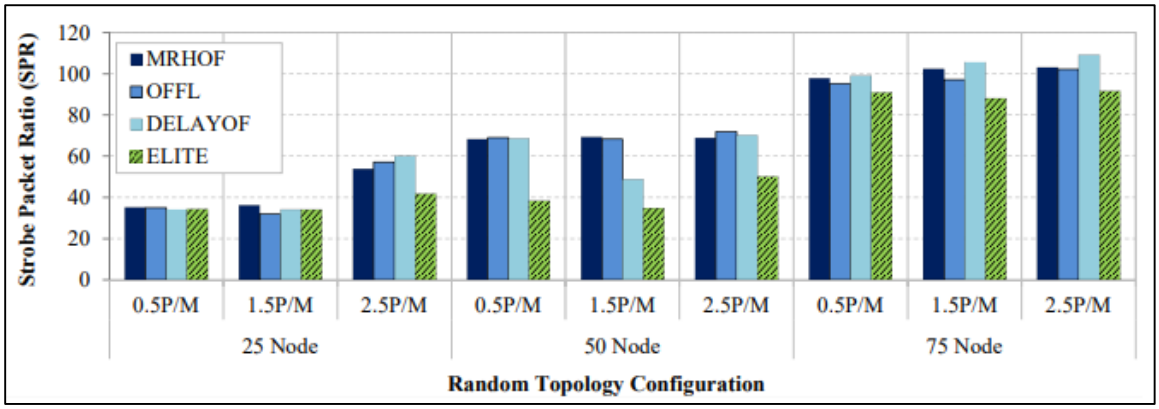

Figure 12 Number of Transmitted Strobes in Each Node in Various Network Scenarios [34]

The author in [36] proposed a new cross-layer-based energy optimization algorithm (CLEOA) for use with a combined AI and mIoT platform. This CL mechanism is created along with specific parameters by considering four layers. The transferring and receiving routes are connected through a wireless channel. An on-body sensor node has a time limit of T to transfer X bits. Sensor nodes monitor the duty-cycle of devices at the MAC layer, $T_{act} \leq T$ by transferring the data to the receiver node whereas the whole duty cycle is calculated as:

$$D_{cycle} = T_{act}/T_{tot}$$

Additionally, in order to obtain an efficient sustainable mIoT platform, transmit and receive power, and data rate is monitored at the network and physical layer. P_{tot} is defined in equations (2) and (3),

$$P_{tot} = P_{act} + P_{slp} = \frac{E_{act}}{T_{act}} + \frac{E_{slp}}{T_{slp}} + \frac{E_{tran}}{T_{tran}} \quad (2)$$

Equations (2) and (3) represented the Power drain problem. Now, they need to optimize *P* Subject to:

$$0 \leq D_{cycle} \leq 1 \quad (3)$$

$0.1\ n \leq d \leq 1\ n$

The major challenge is to optimize energy absorption and improve efficiency by correctly modifying the performance metrics at the MAC layers, application, network, and physical layer. Sensor mIoT nodes execute the different tasks by using the suggested CLEOA. The key objective of the suggested CLEOA is to create a sustainable, reliable, and energy-efficient healthcare platform. In addition, the M-QAM modulation method allows the transition and analysis of broad and error-free healthcare results. In comparison, the D_{c_opt} duty-cycle optimization at the MAC layer greatly decreases the energy drain with better efficiency at the physical layer. The 3GPP has proposed a new IoT technique NB-IoT. It is based on LPWAN radio technology. This technology was developed to provide better coverage and very low power consumption than traditional LTE. This specification implements PSM and eDRX mechanisms for longer battery life [37].

Energy efficiency methods used in IoT environments were suggested by the author in [38]. These techniques have been classified on the basis of five distinct layers of IoT energy architecture. The layers are the local processing and storage layer, sensing layer, cloud processing and storage layer, application layer, network/communication layer.

- Sensing Layer: Three sub-categories; Modulation techniques, Energy Efficient Sleep/Wakeup, Self-Organized Things (SoT)-Based Technique.
- LPSL Layer: Two sub-categories; Cognitive Ratio-Based Techniques, Energy Harvesting.
- NCL Layer: Three sub-categories; Energy Efficient Scheduling, Routing, Communication Techniques.
- CPS Layer: Two sub-categories; Lyapunov Optimization, Virtual Machine Optimization.
- Application Layer: Application-oriented, no subcategories in this layer.

Table 1 classifies and provides qualitative analysis on energy efficiency related to IoT perspective. Various issues and solutions used for energy-efficient techniques have been analyzed in [38].

SURVEY ARTICLE

Layer	Sub-Layer	Reference Paper	Issues	Proposed Solutions
Sensing Layer	Modulation	[40]	- Energy optimization due to unique system restriction through ultra-small system dimension	- Provide optimized and efficient use of energy
	Sleep/Wakeup	[41]	- Energy consumption and data quality management problem	- Optimized energy usage and QoI based solution
		[42]	- Issue of more power consumption and less reliability due to pipeline leakages	- Energy-efficient and robust solution
	SoT	[43]	- More interaction between humans and machines and increased energy usage	- Optimized energy usage, self-managed and durable solution
Local Processing/ Storage Layer	Cognitive Radio Based method	[44]	- More power usage and lack of bandwidth	- Reliable solution with higher throughput.
	Energy Harvesting Layer	[45]	- Wastage of power in overhearing, idle, collision, retransmissions, and listening	- Restricted battery solution
		[46]	- Excess power usage in sleeping, receiving, idle listening, and transmitting	- Provide optimized energy usage and QoS based solution
		[47]	- Restriction on available energy	- Regulation by the use of stored energy and deficient energy to control load
Network/ Communication	Routing Layer	[48]	- Power consumption challenge in asynchronous communication	- Improved lifetime and a lesser amount of energy consumption
		[49]	- Energy consumption and network partitioning in the distributed network	- Uniformly usage of energy by every node and improved network lifespan
		[50]	- Limitation of sensor nodes in the context of power, memory, and processing	- Consistently distribution of network resources, QoS, and improved lifespan
	Scheduling	[51]	- Maintain trade-offs between power usage and QoS.	- Optimized energy usage and Qos based solution for industrial applications
	Communication	[52]	- More latency, small capacity, and sensitive to environmental constraints through diffusion	- Optimized the energy efficiently over long distances and delay-sensitive communication
		[53]	- Poor network design, processing, and resource management	- Provide the energy-efficient solution in a dynamic environment
Cloud Processing and Storage	Lyapunov Optimization	[54]	- Rising CPU and power usage in mobile device	- Provide energy-efficient and properly scheduled solutions with low latency
	Virtual Machine Optimization Layer	[55]	- Challenge to maintain the balance of system performance and power usage	- Provide optimized energy usage and adaptive solution
		[56]	- Energy consumption and high cloud provider cost	- Energy-efficient and robust solution based on consolidation

SURVEY ARTICLE

Application Based		[57]	- Energy consumption, delay	- Green and reliable communication
		[58]	- Uniformly distributed energy consumption	- Scalable and energy-efficient solution

Table 1 Various Issues and Solutions Used for Energy-Efficient Techniques at Different Layers in IoT [38].

Proposed protocol	Issues	Proposed Solution
SMRF[62]	- Absence of support for upward multicast - Can provoke a high end-to-end delay	- Adopt cross-layer optimization to improve multicast forwarding using trickle
BMRF[63]	- Relatively high consumption of memory - Raises end-to-end delay - Adjusting incorrect parameters can cause poor performance	- Combines RPL and SMRF characteristics and improves both upward multicast data forwarding and downward multicast data forwarding - Reduce the power consumption - Increase the PDR
ESMRF[64]	- Difficult and costly in a big routing tree - Inducing communication overhead and raises end to end delay	- Resolves the SMRF gap by enabling both upward multicast data forwarding and downward multicast data forwarding
Co-RPL[65]	- Needs modifications in the RPL messages - Involves the routing table expansion	- Based on the corona mechanism, the routing approach is used to enhance RPL mobility support - Reduces the PLR, energy consumption and delay
MT-RPL[66]	- Dependent on the existence of a fixed node	- Cross-layer protocol between the MAC and routing layers decreases the disconnection time, increases the PDR thereby decreasing the consumption of energy
MRPL[67]	- Small increments in the duration of control messages - Raises the number of control messages exchanged	- It combines the smart-hop mechanism with RPL to provide an easy and efficient mobility support
EC-MRPL[68]	- RSSI value may be affected due to some obstacles in environments so that it is better to enhance the prediction method for better network performance	- Cross-layer approach is used to enhance the routing process in the form of node mobility through estimating the node's movement based on RSSI
EKF-RPL[69]	- Raises end-to-end delay - Does not take into account the significant information like energy and link quality in the selection of parent	- It minimizes the energy consumption and signaling overhead of mobile nodes - It increases PDR
Mod-RPL[70]	- Restriction on the usage of mobile nodes in place of routers and allowed only slow mobile nodes	- Decreases the use of control messages
BRPL[71]	- Significantly increases the delay	- To adaptively distribute the network resources, it integrates RPL with backpressure routing concepts - Provides a substantial decrease in packet losses
EMA-RPL[72]	- Mobile nodes are unable to route other node packets	- It minimizes the power and computing service use of mobile devices

SURVEY ARTICLE

MARPL[73]	- Packet loss in the link-layer can reduce the PDR in all evaluated protocols	- Cross-layer technique used to offer a mobility detection standard
RPLca+[74]	- Provides implementation overhead - Increases the power consumption	- Cross-layer technique is used for link quality prediction and routing table management
EAOF[75]	- Packet delivery rate is decreased	- They used a hybrid approach that is based upon the cross-level emulation and simulation tool - Mitigates power consumption - Increases the network lifespan
FUZZY OF[76]	- Memory usage can be extended by applying a fuzzy system - The concept of fuzzy parameters is not irrelevant and can have a direct effect on network performance	- They used a cross-layer approach to get ETX and delay from DLL and network layers - Decreases PLR - Decreases the end-to-end latency
SCAOF[77]	- Complex approach - Needs an extended version of RPL	- SCAOF is tested with Cooja and analyzed in a hardware testbed for cross-level simulation, in which practical scenarios of the wireless network can be applied more accurately - Enhances network lifespan

Table 2 Routing Solutions for IoT/LLNs [61].

Another energy-efficient solution proposed three layers which are sensing, processing the data, and presenting those data. This method can predict sleep timing to save energy based on historical data and power in batteries of different sensors. Using this technique re-provisioning can be done during the sleep mode of those devices to provide a more energy-efficient solution [39].

4.2. Mobility Issues

Mobility provides several benefits in the form of flexibility, adding more services, and then extending IoT's application domains [59]. Still, it remains a serious problem that needs to be properly handled like the infrequent connection of mobile nodes and nodes disconnection. Data losses and transmission delays are significant issues caused by these disconnections [60]. Hence, by seeking an appropriate connection point in a short and limited time, it is essential to cope with mobility to solve the problems faced and allow continuous communication and connectivity with mobile nodes (MNs).

4.2.1. Existing Solutions

The development of an appropriate mobility support protocol for IoT remains a critical and difficult task. It is only due to the restricted resources of the devices, the inconsistent movements of devices, and the application requirement in terms of the QoS in some areas. Hence, numerous relevant solutions have been suggested to solve these problems under the mobility scenario. Mobility and hop-by-hop transmission require an adaptable routing protocol to manage frequently changing topologies. The LLN routing protocol should include efficient methods for rapid mobility identification. It can help to reduce packets loss due to system mobility and mitigate disconnection consequences. RPL is a proactive routing protocol. It generates acyclic graphs connecting the nodes to enable the sharing of data. It was originally intended for static LLN topologies but it has certain limitations and disadvantages. It faces a series of issues when dealing with mobility, including the lack of a mobility identification system and the inability to detect or prevent link disconnection. Several routing models have been suggested to deal with the lack of mobility support for RPL [61]. Table 2 summarizes routing solutions for IoT.

4.3. Adaptability and Interoperability Between the Layers

The concept of interoperability can already be described as the capability of two systems to interact and exchange resources with each other. One of the main aims of IoT is to achieve interoperability. But it has become a difficult thing and a research issue.

Lack of interoperability causes many critical issues like the impossibility of plugging non-interoperable IoT devices into heterogeneous IoT platforms, the complexity of developing IoT applications using several uniforms and/or cross-domain platforms, the avoidance of large-scale implementation of IoT technology, discouragement of the implementation of IoT technology, cost increases, minimum reusability, and user disappointment.

SURVEY ARTICLE

4.3.1. Existing Solutions

Over the previous few years, research has shown a tremendous increase in the number of solutions available for a wide variety of devices and IoT platforms. However, each approach offers its own IoT systems, devices, data formats, and functionalities that lead to the problems of interoperability. In terms of the various methodology associated with energy efficiency, mobility, quality of service, and security, the cross-layer interoperability makes IoT framework progressively compelling and effective in different applications. Figure 13 illustrates the concept of interoperability in IoT layers.

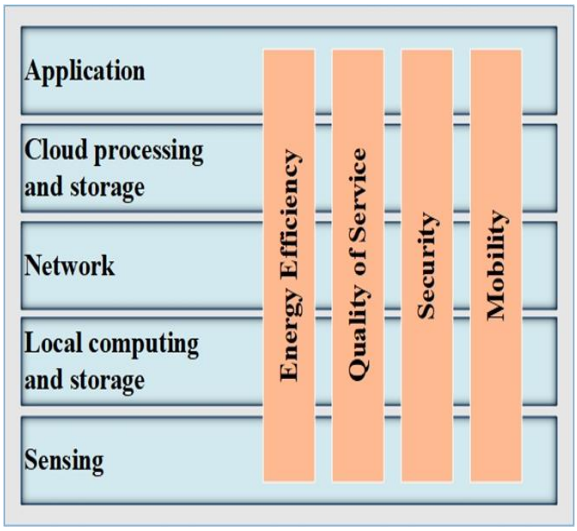

Figure 13 Cross-Layer Interoperability [38].

The symbIoTe is an H2020 research and innovation project. Its main goal is to solve the challenging task of an IoT environment that is interoperable. It allows the coordination of vertical IoT platforms in order to create cross-domain applications. Figure 14 illustrates the symbIoTe architecture.

The Application Domain layer enables collaboration by providing a high-level API with a unified view across various platforms. It promotes cross-platform management and discovery of IoT tools including the acquisition and execution of data in compliance with platform-specific business rules. The Cloud Domain layer includes the cloud-adjusted modules of individual platforms. The Smart Space Domain is made up of smart objects, IoT gateways along with storage resources, and local computing. symbIoTe middleware enables the discovery and reconfiguration of smart devices, platform interoperability, and component-based smart object roaming. Smart objects in the device domain can be self-organized and can be designed on the fly to be embedded within the smart space with numerous IoT platforms. It prevents customers from locking into a particular IoT platform and IoT provider [78]. Thus, symbIoTe is addressed as an important interoperability mechanism. Now in [79], the author has presented new aspects of interoperability in organizations. These are relevant to federations of IoT platforms, SLA and trust management, the concept of resource bartering along roaming IoT devices.

Resolving IoT Interoperability Gap (BIG IoT) is an IoT-EPI project designed to allow cross-platform, cross-standard, and cross-domain IoT services and applications to be developed in order to build an IoT ecosystem. These IoT ecosystems are relating things and service providers and their customers [80].

The author proposed a high-level IoT interoperability architecture based on an open cross-layer system in [81]. It enables interoperability between heterogeneous cross-domain IoT platforms. It helps to connect already deployed or newly implemented IoT systems and facilitates the connection of every application area across various IoT domains. Figure 15 shows the high-level architectural model that allows cross-domain interoperability between heterogeneous IoT platforms.

This open IoT framework offers a common platform with high-level APIs to facilitate collaboration and promote cross-domain discovery and management of IoT resources from various platforms. To address the lack of interoperability, a multi-layered INTER-IoT approach was proposed by the author in [82]. Its main objective is to offer open IoT interoperability, which provides the ability to connect and collaborate with manufacturers and developers, without competing with anyone and succeed by providing a good service and experience. INTER-IoT aims to establish CL interoperability and integration across heterogeneous IoT platforms. CL methods are essential for the entire layered stack of IoT systems to be interoperable/integrated. In addition, significant specifications and functions like QoS, QoE, Protection, Confidence, and Safety need to be handled at every layer with various methods.

Different standardization projects are currently ongoing to explain architectural standards for interoperability with IoT domains. IoT-EPI projects are designing interoperability mechanisms that are discussing different layers of the IoT architecture and provide interoperability solutions between various IoT. Table 3 explains some important IoT-EPI projects.

4.4. Security Issues

One of the main concerns in IoT is the security issue. In IoT applications, data loss and breach of many other purposes of the data has been occurred because of weak codes or non-encrypted systems. So, IoT applications need to be made more secure both internally and externally. Security techniques should be employed in all the layers and also when the data is being transferred from one device to another device [84]. All the devices in IoT systems have different capabilities

SURVEY ARTICLE

and various specifications leading to a heterogeneous nature. So in environments like this security is more important as the chances of devices getting hacked by intruders are high. To protect the user's privacy, each device must employ authentication and encryption mechanisms [85]. The security at different layers are discussed below:

- Perception Layer - The main security issue related to this layer is that the flow of signals from one point to another is affected by the waves. So the signals lack the power required to transmit the information which presents a big challenge for communication. During transmission, the intruders can manipulate the hardware part of the devices and the signal can be changed. The transmission of information from subsequent sensors comes under problems leading to network complications and will affect smooth communication [86].

- Network Layer - IoT devices are diverse in nature which makes it easy for the attackers to use the traffic of the channel and fetch the private data. The attacker can manipulate data and information to their personal interests leading to negative implications in IoT devices [87]. Network systems should meet the compatibility criterion that enables them to exchange information in the required manner.

- Application layer -There are various applications in IoT and each application follows its own way to maintain the confidentiality of the data. Also, the approach of authentication within networks varies from every system making it ineffective. For example, a network system with different coding patterns influences the authentication procedures used will create problems in sharing and accessing information [88]. This creates a problem in applications for transmitting the data in the required time.

4.4.1. Existing Solution

The cross-layer design in IoT security issues has many solutions that are cryptographic algorithms, secure routing, key management, and node trust. The main way of ensuring security to IoT devices is through encryption. Usage of cross-layer model provides additional security by deploying some encryption techniques.

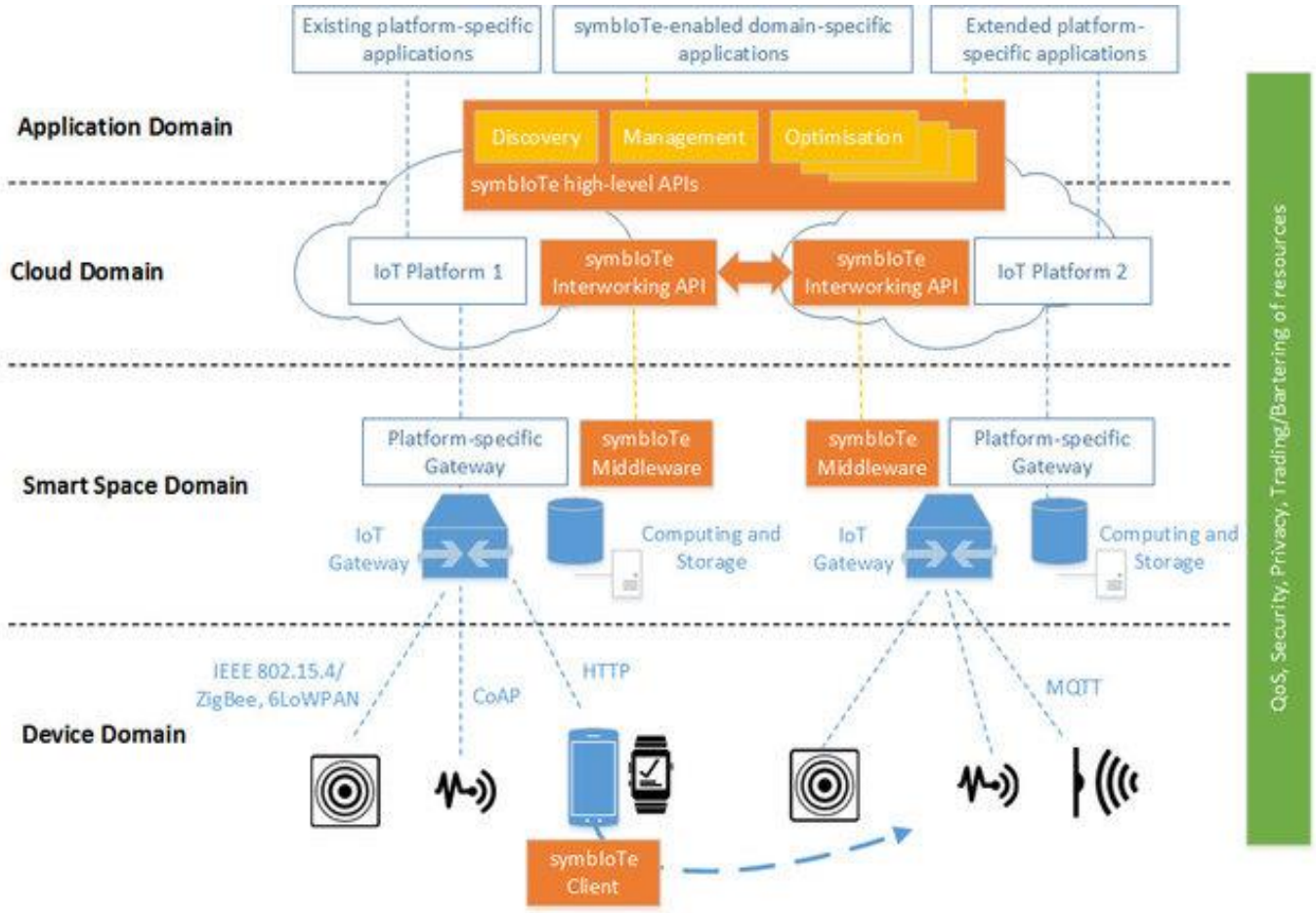

Figure 14 symbIoTe Architecture [78]

SURVEY ARTICLE

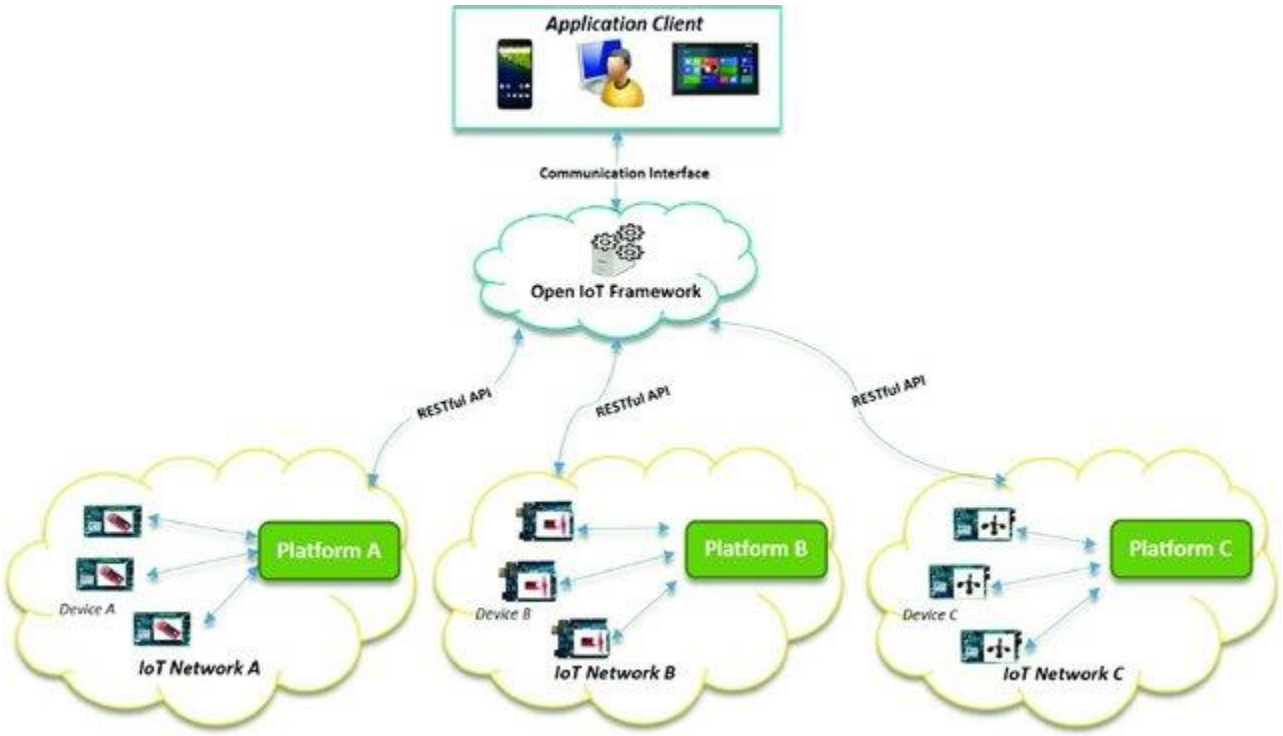

Figure 15 Interoperability Architecture Model for Cross-Domain IoT Platforms [81].

IoT-EPI projects	Objective	Issues Identified by INTER-IoT
BIG IoT	It develops interoperability through specifying unified Web API for IoT platforms. It emphasizes the upper layers of IoT architecture by describing the APIs, security management, external system services, service integration, applications, and the commercial enterprise.	This approach provides a higher-level API to allow application and service interoperability. It does not include any IoT platform integration methods and methodologies for the various fine-grain layers defined by INTER-IoT
AGILE	Its primary purpose is to solve technological and syntactic interoperability at the level of hardware and software. Hardware-level modules provide support for multiple technologies like wireless and wired IoT networking. Software modules cover functions including device management, security management of communication networks, and distributed storage solutions.	This approach provides interoperability with the device layer. It does not include any IoT platform integration methods and techniques for the various fine-grain layers described by INTER-IoT.
symbIoTe	It allows the discovery and resource sharing for the rapid development of cross-platform application technologies. It enables the integration of smart objects with surrounding environments. By developing and integrating an Open Source mediation prototype, symbIoTe can achieve both of the above.	This method is typically built on a mediation prototype to facilitate interoperability. It does not include IoT platform integration methods and methodologies for the various fine-grain layers defined by INTER-IoT

SURVEY ARTICLE

TagItSmart	It provides a variety of tools and enables technologies that can be embedded into various IoT platforms using available APIs. It helps customers through the supply chain to completely leverage the power of condition-dependent functional codes to link mass-market goods across multiple application sectors to the digital environment.	This approach is not designed for heterogeneous IoT interoperability. Systems focused on the methods and methodologies of integration/interconnection.
VICINITY	It focuses on a platform and design for IoT systems that offer "interoperability as a service". The work that takes into consideration is system automation, business logic, virtualization, infrastructure, APIs, tools, external system resources, software, cloud services, and data processing.	In general, this approach focuses on infrastructure gateways to facilitate interoperability. It does not provide techniques and methodologies for IoT platform integration for various fine-grain layers defined by INTER-IoT.
bIoTope	It provides the appropriate open standard APIs to allow heterogeneous information sources and resources from various channels, like city dashboards, OpenIoT, FI-WARE, etc., to be written, consumed and composed [83].	This approach provides a higher-level API to allow device interconnection systems. It does not include any IoT platform integration methods and methodologies for the various fine-grain layers defined by INTER-IoT.

Table 3 Some Important IoT-EPI Projects [82].

4.4.2. Encryption

The data shared among IoT devices and the cloud service should be securely encrypted to preserve user privacy and sensitive information. Although, traditional encryption schemes offer strong security assurance. Even then, it's also difficult to implement them to resource-restricted devices. NIST defined a variety of lightweight cryptography approaches for solving this problem [89]. They described various lightweight cryptography primitives which are presented in Table 4.

4.4.3. Trust Management (TM)

In IoT, TM contributes a major part in efficient data fusion and data mining, qualified services, and improved data security and user privacy. It allows users to resolve expectations of uncertainty and vulnerability. It includes user acceptance and usage of IoT resources and technologies. The author in [90] presented a comprehensive trust management framework of IoT. It includes cross-layer and inter-layer IoT TM and modules for providing functional and intelligent IoT applications and services focused on trustworthy social trust relationships. The author in [91], presented a cross-layer security monitoring selection algorithm (CLSM) that is based on traffic prediction (TP). So, they selected the monitoring node with a relatively high idle degree by estimating the traffic of the node based on a CL VANET. In addition, the shared data and residual energy were used by this algorithm to optimize the collection of nodes by social network analysis. It can balance the consumption of energy between all nodes and enhance the lifespan of VANET to some level.

In [92] the author suggested the Cross-Layer Security Approach integrated security laws into events and allow the network to reroute events, policies, and specific requirements of publishers. It helps to enhance the efficiency of the system while retaining IoT service interaction functionality and simultaneously minimizing the visibility of the event. The complexities of protecting event-driven IoT services have been resolved by this cross-layer security architecture for NBN (notification broker network).

A cross-layer security system was designed in [93] to ensure the security of all IoT layers. In IoT attacks, like DoS attacks, some malicious attacks can infect IoT layers. Therefore, the CLD is assumed appropriate for adequate security solutions. The cross-layered solution requires communication in all layers with all components and the huge number of IoT-related objects that trigger big data challenges. Thus, cross-layer technologies combined with a big data cluster module can improve security agents in IoT environments.

Figure 16 demonstrates the cross-layer scenario, big data cluster, and decision making. ADD can detect attacks in the application layer by collecting data from ADD1-n. It is an application-based attack detector and transmitting data to big data analytics. NAD is capable of transferring network layer data to big data analytics. SAD can transfer physical layer data to a big data cluster. The short-term data among the applications layer and sensors layer can be detected by the ADD1-n, SAD1-n. Once the data is analyzed using the big data cluster module for a specific traffic type then the output is transferred to the decision-making module.

SURVEY ARTICLE

Cryptographic Algorithm	Block Size	Key Size	No. of Round	Structure
AES	128	128/192/256	10/12/14	SPN*
PRESENT	64	80/128	31	SPN
HEIGHT	64	128	32	GFS+
RC5	32/64/128	02040	1255	Feistel-
LEA	128	128,192,256	24/28/32	Feistel
TEA	64	128	64	Feistel
DES	64	54	16	Feistel
Iceberg	64	128	16	SPN
DESL	64	54	16	Feistel
3DES	64	56/112/168	48	Feistel
Twine	64	80/128	32	Feistel
Hummingbird	16	256	4	SPN
Hummingbird2	16	256	4	SPN
XTEA	64	128	64	Feistel
Pride	64	128	20	SPN

Table 4 Various Lightweight Cryptographic Algorithms [89].

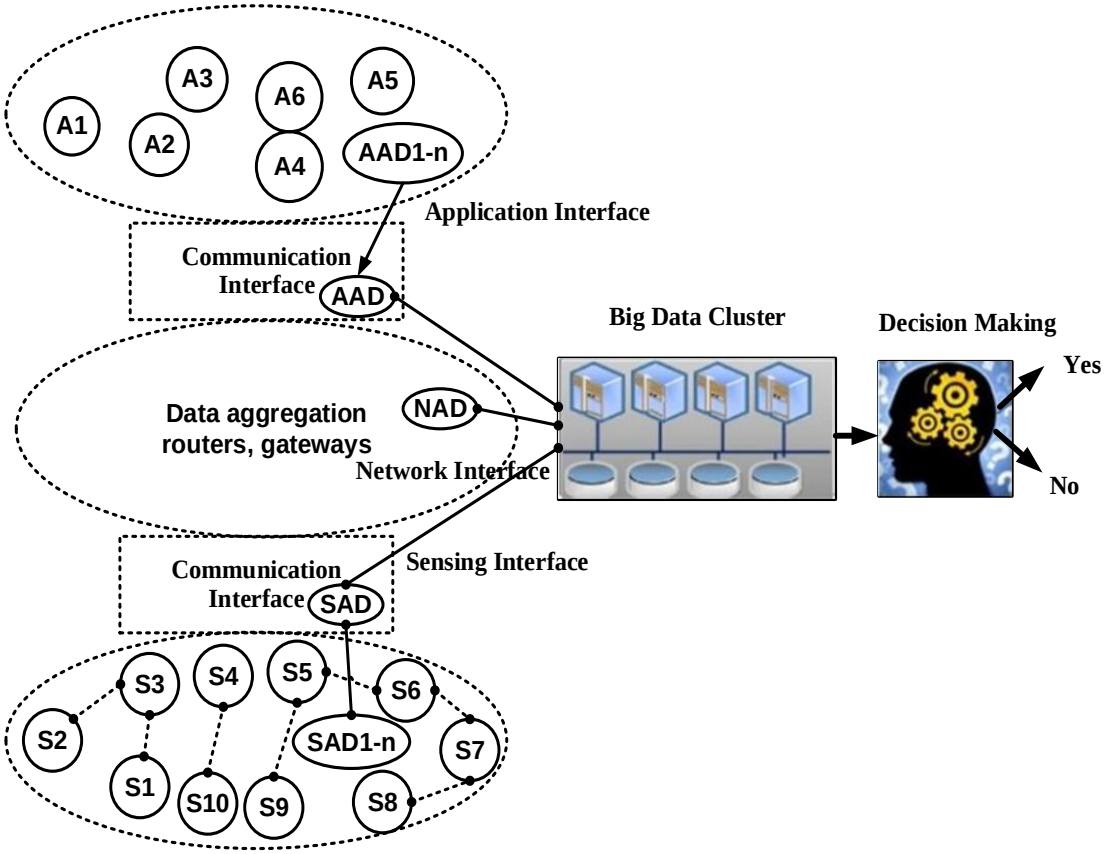

Figure 16 Cross Layer Scenario [93].

SURVEY ARTICLE

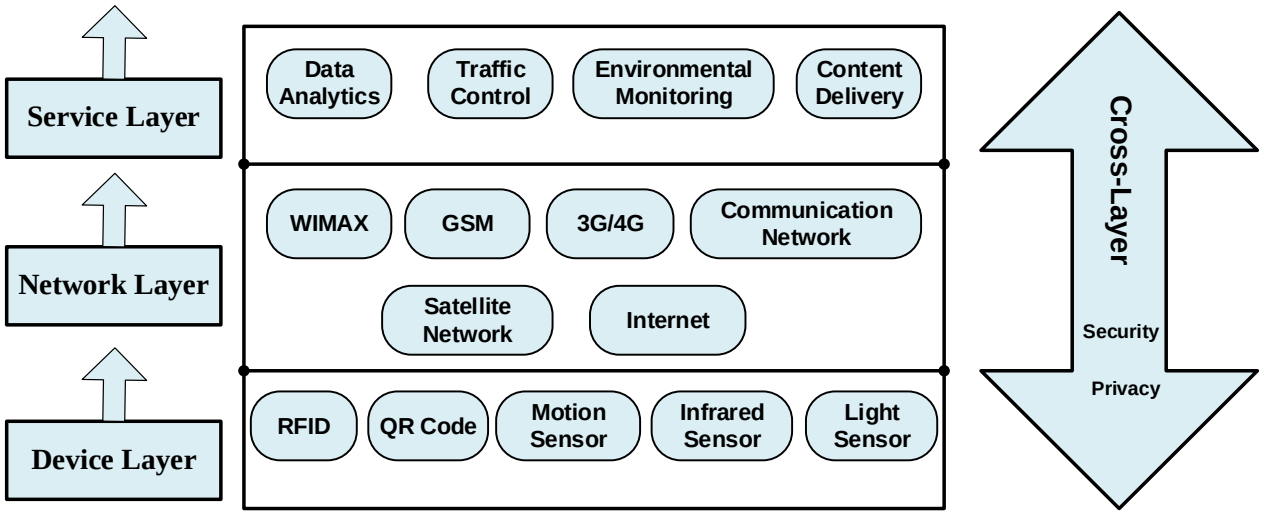

Figure 17 A Standard Layered Architecture of IoT Platforms [94].

A cross-layer framework to secure IoT systems is suggested by the author in [94]. To achieve security XLF is intended to use observations into adverse capabilities and system properties at various layers. XLF is composed of a collection of building blocks that may be deployed on a device or a network, as well as in the cloud or through a service provider's gateway. Figure 17 shows a standard layered architecture of IoT platforms.

4.5. Privacy and Scalability

In the future, privacy is more important as all our information is going to be available on all our smart devices. The increased usage of smart devices will be a challenging one to provide security for it. For example, the smartphone is developed for single-person usage which contains all the private information which should be highly secured. Some of the foreseen challenges include security issues, privacy issues as well as scalability. The security issue stretches to other aspects like standardization and networking of the same.

4.5.1. Existing Solutions

CLD can be used to resolve the issues in privacy and to provide confidentiality and security. In CLD, non-repudiation is required for authorization and authentication. The authentication and data confidentiality in IoT devices is made by encapsulation of data. Datagram transport layer security protocol is used for authentication in IoT devices with the help of CLD. So a two-way authentication model is designed to provide better privacy and scalability.

Conventional authentication methods are not efficient in terms of overhead for IoT devices. However, they are appropriate for authenticating devices that transmit streaming data. As a result, a simplified authentication mechanism is critical for large-scale IoT devices. Cross-layer authentication might be considered a possible approach that combines the benefits of PLA and cryptography-based authentication.

Existing approaches of cross-layer authentication methods in [95] [97] do not take signaling overhead and authentication performance into account. The performance of the cross-layer authentication method has not been thoroughly investigated. The author in [95] suggested a cross-layer authentication approach in order to reduce latency in smart meter systems. However, it lacks the authentication reliability associated with cryptography-based authentication. Cross-layer authentication protocols [96] [97], on the other hand, are unable to reduce overhead and delay, while PLA and cryptography-based authentication would increase authentication performance. As a result, the author in [98] devised a low-level cross-layer authentication scheme.

Table 5 shows the abbreviations used in this paper.

Abbreviation	Description
ELITE	Elaborated Cross-Layer RPL Objective Function to Achieve Energy Efficiency
BLE	Bluetooth Low Energy
DELAYOF	Delay Objective Function
MRHOF	Minimum Rank Hysteresis Objective
RFID	Radio-Frequency Identification
CL	Cross-Layer
PSM	Power saving mode
Edrx	Extended Discontinuous Reception
NCL	Network communication layer
LLN	Low-power and Lossy Networks
IoT-EPI	IoT-European Platforms Initiative
ICT	Information and Communication
QoE	Quality of Experience
XLF	Cross-Layer Framework
NIST	National Institute of Standards and

SURVEY ARTICLE

LTE	Long-Term Evolution
UDDI	Universal Description, Discovery, and
SAD	Sensor layer attack detector
NAD	Network layer attack detector
PLA	Physical layer authentication

Table 5 Abbreviations Used in the Paper

4.6. The Problem of Fragmentation and Reassembly in 6LoWPAN

In 6LoWPAN, the relatively large IPv6 packet is fragmented so that it may be efficiently transported by a small size IEEE 802.15.4 frame. It is possible to redirect corresponding fragments to the destination with the help of multi-hops route-over routing protocols. PDR is high with the traditional route-over routing protocol. It suffers from high average latency as a result of hop-by-hop fragmentation and reassembly. Additionally, the enhanced route-over routing eliminates the average latency by avoiding hop-by-hop fragmentation and reassembly. Although, enhanced route-over has adverse effects of low PDR and throughput particularly when the route has a large number of hops and packet fragments.

4.6.1. Existing Solution

An adaptive exponential backoff technique has been implemented using CLD between IEEE 802.15.4 MAC and 6LoWPAN adaptation layers. The backoff exponent parameters MinBEc and MaxBEc are implemented in this protocol based on the number of fragments. As a result, inter fragment interference reduces collisions and conflicts between intermediate forwarders. The adaptation layer defines and integrates the number of fragments into the header of the adaptation layer [99].

5. CONCLUSION

To make the IoT system efficient CLD can be used to further improve several aspects of IoT. In this paper, the evolution, taxonomy of architecture, communication technologies, and applications of IoT has been discussed in detail. The Cross-Layer Design of WSN in the context of IoT was also discussed. Various suggested CLDs if integrated with IoT, have various problems that were addressed based on several issues in security, privacy, mobility, interoperability, and energy consumption. A number of possible solutions have been discussed in this paper but there is still a necessity for various measures that can be used to overcome IoT-related challenges. The future belongs to IoT as the recent study showed that the steady rise in the growth of IoT-connected devices would be more in billions, so the problems need to be addressed so that a far efficient system can be formed.

REFERENCES

[1] Xu, Lina, Anca Delia Jurcut, and Hamed Ahmadi. "emerging Challenges and Requirements for internet of things in 5G." In 5G-Enabled Internet of Things, pp. 29-48. CRC Press, 2019.

[2] Hassan, Qusay F., ed. “Internet of things A to Z: technologies and applications.” John Wiley & Sons, 2018.

[3] B. TORĞUL, L. Şağbanşua, and F. B. Balo, “Internet of Things: A Survey,” Int. J. Appl. Math. Electron. Comput., no. March, pp. 104–104, 2016.

[4] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.

[5] H. Machado and N. Lane, “Internet of Things (IoT) impacts on Supply Chain,” APICS Houst. Student Chapter, vol. 77007, no. 402, pp. 2493–2498, 2014.

[6] S. Madakam, R. Ramaswamy, and S. Tripathi, “Internet of Things (IoT): A Literature Review,” J. Comput. Commun., vol. 03, no. 05, pp. 164–173, 2015.

[7] Jiang, Lihong, Li Da Xu, Hongming Cai, Zuhai Jiang, Fenglin Bu, and Boyi Xu. "An IoT-oriented data storage framework in cloud computing platform." IEEE Transactions on Industrial Informatics 10, no. 2 (2014): 1443-1451.

[8] Goyal, Krishan Kumar, Amit Garg, Ankur Rastogi, and Saurabh Singhal. "A literature survey on Internet of Things (IoT)." International Journal of Advanced Networking and Applications 9, no. 6 (2018): 3663-3668.

[9] M. Ahmad, T. Younis, M. A. Habib, R. Ashraf, and S. H. Ahmed, “A Review of Current Security Issues in Internet of Things,” pp. 11–23, 2019.

[10] Jan, Mian Ahmad, Fazlullah Khan, and Muhammad Alam, eds. “Recent trends and advances in wireless and IoT-enabled networks” Springer, 2019.

[11] https://www.netburner.com/learn/architecturalframeworks-in-the-iot-civilization

[12] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” J. Electr. Comput. Eng., vol. 2017, 2017.

[13] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, “IoT elements, layered architectures and security issues: A comprehensive survey,” Sensors (Switzerland), vol. 18, no. 9, pp. 1–37, 2018.

[14] Saadeh, Maha, Azzam Sleit, Khair Eddin Sabri, and Wesam Almobaideen. "Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities." Journal of Network and Computer Applications 121 (2018): 1-19.

[15] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017.

[16] S. Kraijak and P. Tuwanut, “A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends,” Int. Conf. Commun. Technol. Proceedings, ICCT, vol. 2016-Febru, pp. 26–31, 2016.

[17] J. Kaur and K. Kaur, “Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends,” Int. J. Comput. Netw. Inf. Secur., vol. 9, no. 4, pp. 57–70, 2017.

[18] Al-Sarawi, Shadi, Mohammed Anbar, Kamal Alieyan, and Mahmood Alzubaidi. "Internet of Things (IoT) communication protocols." In 2017 8th International conference on information technology (ICIT), pp. 685-690. IEEE, 2017.

[19] V. Bhuvaneswari and R. Porkodi, “The internet of things (IOT) applications and communication enabling technology standards: An overview,” Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014, no. October 2017, pp. 324–329, 2014.

[20] P. P. Ray, “A survey on Internet of Things architectures,” J. King Saud Univ. - Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, 2018.

[21] P. Bhoyar, P. Sahare, S. B. Dhok, and R. B. Deshmukh, “Communication technologies and security challenges for internet of things: A comprehensive review,” AEU - Int. J. Electron. Commun., vol. 99, pp. 81–99, 2019.

[22] H. D. Kotha and V. Mnssvkr Gupta, “IoT application, a survey,” Int. J. Eng. Technol., vol. 7, no. May, pp. 891–896, 2018.

SURVEY ARTICLE

[23] S. Parween and S. Z. Hussain, "A review on cross-layer design approach in WSN by different techniques," Adv. Sci. Technol. Eng. Syst., vol. 5, no. 4, pp. 741–754, 2020.
[24] B. Fu, Y. Xiao, H. J. Deng, and H. Zeng, "A survey of cross-layer designs in wireless networks," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 110–126, 2014.
[25] C. Luo, F. R. Yu, H. Ji, and V. C. M. Leung, "Cross-layer design for TCP performance improvement in cognitive radio networks," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2485–2495, 2010.
[26] G. Shine Let and G. Josemin Bala, "A review of cross-layer design in dynamic spectrum access for cognitive radio networks," J. Comput. Inf. Technol., vol. 22, no. 1, pp. 21–29, 2014.
[27] Mashal, Ibrahim, Osama Alsaryrah, Tein-Yaw Chung, Cheng-Zen Yang, Wen-Hsing Kuo, and Dharma P. Agrawal. "Choices for interaction with things on Internet and underlying issues." Ad Hoc Networks 28 (2015): 68-90.
[28] W. Wang, S. De, and A. Lehmann, "Semantic description framework for IoT services," EC FP7 Project IoT.est, 2012.
[29] B. Jia, S. Liu, and Y. Yang, "Fractal cross-layer service with integration and interaction in internet of things," Int. J. Distrib. Sens. Networks, vol. 2014, 2014.
[30] S. Alam and J. Noll, "A semantic enhanced service proxy framework for internet of things," Proc. - 2010 IEEE/ACM Int. Conf. Green Comput. Commun. GreenCom 2010, 2010 IEEE/ACM Int. Conf. Cyber, Phys. Soc. Comput. CPSCom 2010, pp. 488–495, 2010.
[31] Z. Song, A. A. Cárdenas, and R. Masuoka, "Semantic middleware for the internet of things," 2010 Internet Things, IoT 2010, 2010.
[32] A. Tandon and P. Srivastava, "Location based secure energy efficient cross layer routing protocols for IOT enabling technologies," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 7, pp. 368–374, 2019.
[33] F. Yu, V. Krishnamurthy, and V. C. M. Leung, "Cross-layer optimal connection admission control for variable bit rate multimedia traffic in packet wireless CDMA networks," IEEE Trans. Signal Process., vol. 54, no. 2, pp. 542–555, 2006.
[34] B. Safaei, A. M. H. Monazzah, and A. Ejlali, "ELITE: An Elaborated Cross-Layer RPL Objective Function to Achieve Energy Efficiency in Internet of Things Devices," IEEE Internet Things J., vol. X, no. X, pp. 1–1, 2020.
[35] A. Dunkels, F. Osterlind, N. Tsiftes, and Z. He, "Software-based on-line energy estimation for sensor nodes," Proc. 4th Work. Embed. Networked Sensors, EmNets 2007, pp. 28–32, 2007.
[36] A. H. Sodhro, M. S. Obaidat, S. Pirbhulal, G. H. Sodhro, N. Zahid, and A. Rawat, "A novel energy optimization approach for artificial intelligence-enabled massive internet of things," Proc. 2019 Int. Symp. Perform. Eval. Comput. Telecommun. Syst. SPECTS 2019 - Part SummerSim 2019 Multiconference, 2019.
[37] Sultania, Ashish Kumar, Pouria Zand, Chris Blondia, and Jeroen Famaey. "Energy Modeling and Evaluation of NB-IoT with PSM and eDRX." In 2018 IEEE Globecom Workshops (GC Wkshps), pp. 1-7. IEEE, 2018.
[38] K. Kumar, S. Kumar, O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-layer energy optimization for IoT environments: Technical advances and opportunities," Energies, vol. 10, no. 12, 2017.
[39] N. Kaur and S.K.Sood, "An energy -efficient architecture for the Internet of Things (IoT) ", IEEE Systems Journal, vol. 11, no. 2, pp. 796 –805, 2017.
[40] Y. Chen et al., "Energy-Autonomous Wireless Communication for Millimeter-Scale Internet-of-Things Sensor Nodes," IEEE J. Sel. Areas Commun., vol. 34, no. 12, pp. 3962–3977, 2016.
[41] C. H. Liu, J. Fan, J. W. Branch, and K. K. Leung, "Toward QoI and energy-efficiency in internet-of-things sensory environments," IEEE Trans. Emerg. Top. Comput., vol. 2, no. 4, pp. 473–487, 2014.
[42] R. Du, L. Gkatzikis, C. Fischione, and M. Xiao, "Energy Efficient Sensor Activation for Water Distribution Networks Based on Compressive Sensing," IEEE J. Sel. Areas Commun., vol. 33, no. 12, pp. 2997–3010, 2015.
[43] Ö. U. Akgül and B. Canberk, "Self-Organized Things (SoT): An energy efficient next generation network management," Comput. Commun., vol. 74, pp. 52–62, 2016.
[44] F. F. Qureshi, R. Iqbal, and M. N. Asghar, "Energy efficient wireless communication technique based on Cognitive Radio for Internet of Things," J. Netw. Comput. Appl., vol. 89, pp. 14–25, 2017.
[45] J. H. Ahn and T. J. Lee, "ALLYS: All You Can Send for Energy Harvesting Networks," IEEE Trans. Mob. Comput., vol. 17, no. 4, pp. 775–788, 2018.
[46] T. D. Nguyen, J. Y. Khan, and D. T. Ngo, "Energy harvested roadside IEEE 802.15.4 wireless sensor networks for IoT applications," Ad Hoc Networks, vol. 56, pp. 109–121, 2017.
[47] S. Mondal and R. Paily, "Efficient Solar Power Management System for Self-Powered IoT Node," IEEE Trans. Circuits Syst. I Regul. Pap., vol. 64, no. 9, pp. 2359–2369, 2017.
[48] S. A. Chelloug, "Energy-Efficient Content-Based Routing in Internet of Things," J. Comput. Commun., vol. 03, no. 12, pp. 9–20, 2015.
[49] S. H. Park, S. Cho, and J. R. Lee, "Energy-efficient probabilistic routing algorithm for internet of things," J. Appl. Math., vol. 2014, 2014.
[50] K. Machado, D. Rosário, E. Cerqueira, A. A. F. Loureiro, A. Neto, and J. N. de Souza, "A routing protocol based on energy and link quality for internet of things applications," Sensors (Switzerland), vol. 13, no. 2, pp. 1942–1964, 2013.
[51] Song, Liumeng, Kok Keong Chai, Yue Chen, John Schormans, Jonathan Loo, and Alexey Vinel. "QoS-aware energy-efficient cooperative scheme for cluster-based IoT systems." IEEE Systems Journal 11, no. 3 (2017): 1447-1455.
[52] S. Qiu, W. Haselmayr, B. Li, C. Zhao, and W. Guo, "Bacterial Relay for Energy-Efficient Molecular Communications," IEEE Trans. Nanobioscience, vol. 16, no. 7, pp. 555–562, 2017.
[53] A. Biason et al., "EC-CENTRIC: An Energy- and Context-Centric Perspective on IoT Systems and Protocol Design," IEEE Access, vol. 5, pp. 6894–6908, 2017.
[54] J. Kwak, Y. Kim, J. Lee, and S. Chong, "DREAM: Dynamic Resource and Task Allocation for Energy Minimization in Mobile Cloud Systems," IEEE J. Sel. Areas Commun., vol. 33, no. 12, pp. 2510–2523, 2015.
[55] D. M. Bui, Y. I. Yoon, E. N. Huh, S. I. Jun, and S. Lee, "Energy efficiency for cloud computing system based on predictive optimization," J. Parallel Distrib. Comput., vol. 102, pp. 103–114, 2017.
[56] M. Abu Sharkh and A. Shami, "An evergreen cloud: Optimizing energy efficiency in heterogeneous cloud computing architectures," Veh. Commun., vol. 9, no. February, pp. 199–210, 2017.
[57] A. Liu, Q. Zhang, Z. Li, Y. june Choi, J. Li, and N. Komuro, "A green and reliable communication modeling for industrial internet of things," Comput. Electr. Eng., vol. 58, pp. 364–381, 2017.
[58] T. C. Chiu, Y. Y. Shih, A. C. Pang, and C. W. Pai, "Optimized Day-Ahead Pricing with Renewable Energy Demand-Side Management for Smart Grids," IEEE Internet Things J., vol. 4, no. 2, pp. 374–383, 2017.
[59] Lu´ıs M. L. Oliveira, Amaro F. de Sousa and Joel J. P. C. Rodrigues." Routing and mobility approaches in IPv6 over LoWPAN mesh networks", IJCS, Volume 24, Issue 11, pp 1445-1466, November 2011.
[60] L.Bartolozzi, F.Chiti, R.Fantacci, T.Pecorella & F.Sgri lli, "Supporting monitoring applications with mobile Wireless Sensor Networks: The eN Route forwarding approach", IEEE International Conference on Communications (pp. 5403-5407), Ottawa, Canada, June 2012.
[61] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in internet of things applications," Sensors (Switzerland), vol. 19, no. 9, pp. 1–40, 2019.
[62] Oikonomou, George, Iain Phillips, and Theo Tryfonas. "IPv6 multicast forwarding in RPL-based wireless sensor networks." Wireless personal communications 73, no. 3 (2013): 1089-1116.
[63] G. Gastón Lorente, B. Lemmens, M. Carlier, A. Braeken, and K. Steenhaut, "BMRF: Bidirectional Multicast RPL Forwarding," Ad Hoc Networks, vol. 54, pp. 69–84, 2017.

SURVEY ARTICLE

[64] K. Q. A. Fadeel and K. Elsayed, "ESMRF: Enhanced stateless multicast RPL forwarding for IPv6-based low-power and lossy networks," IoT-Sys 2015 - Proc. 2015 Work. IoT Challenges Mob. Ind. Syst., no. June 2016, pp. 19–24, 2015.

[65] Gaddour, Olfa, et al. "Co-RPL: RPL routing for mobile low power wireless sensor networks using Corona mechanism." Proceedings of the 9th IEEE international symposium on industrial embedded systems (SIES 2014). IEEE, 2014.

[66] C. Cobârzan, J. Montavont, T. Noel, C. Cobârzan, J. Montavont, and T. Noel, "MT-RPL: a cross-layer approach for mobility support in to cite this version: HAL Id: hal-02088111 on Internet of Things EAI Endorsed Transactions MT-RPL: a cross-layer approach for mobility support in," pp. 0–12, 2019.

[67] H. Fotouhi, D. Moreira, and M. Alves, "MRPL: Boosting mobility in the Internet of Things," Ad Hoc Networks, vol. 26, pp. 17–35, 2015.

[68] M. Bouaziz, A. Rachedi, and A. Belghith, "EC-MRPL: An energy-efficient and mobility support routing protocol for Internet of Mobile Things," 2017 14th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2017, pp. 19–24, 2017.

[69] M. Bouaziz, A. Rachedi, and A. Belghith, "EKF-MRPL: Advanced mobility support routing protocol for internet of mobile things: Movement prediction approach," Futur. Gener. Comput. Syst., vol. 93, pp. 822–832, 2019.

[70] Gara, F.; Ben Saad, L.; Ben Ayed, R.; Tourancheau, B. RPL protocol adapted for healthcare and medical applications. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015; pp. 690–695.

[71] Y. Tahir, S. Yang, and J. McCann, "BRPL: Backpressure RPL for High-throughput and Mobile IoTs," arXiv, vol. 2, 2017.

[72] M. Bouaziz, A. Rachedi, A. Belghith, M. Berbineau, and S. Al-Ahmadi, "EMA-RPL: Energy and mobility aware routing for the Internet of Mobile Things," Futur. Gener. Comput. Syst., vol. 97, pp. 247–258, 2019.

[73] J. Kniess and V. de Figueiredo Marques, "MARPL: A crosslayer approach for Internet of things based on neighbor variability for mobility support in RPL," Trans. Emerg. Telecommun. Technol., no. November 2019, pp. 1–17, 2020.

[74] E. Ancillotti, R. Bruno, and M. Conti, "Reliable data delivery with the IETF routing protocol for low-power and lossy networks," IEEE Trans. Ind. Informatics, vol. 10, no. 3, pp. 1864–1877, 2014.

[75] C. Abreu, M. Ricardo, and P. M. Mendes, "Energy-aware routing for biomedical wireless sensor networks," J. Netw. Comput. Appl., vol. 40, no. 1, pp. 270–278, 2014.

[76] P. O. Kamgueu, E. Nataf, and T. N. Djotio, "On design and deployment of fuzzy-based metric for routing in low-power and lossy networks," Proc. - Conf. Local Comput. Networks, LCN, vol. 2015-December, pp. 789–795, 2015.

[77] Y. Chen, J. P. Chanet, K. M. Hou, H. Shi, and G. de Sousa, "A scalable context-aware objective function (SCAOF) of routing protocol for agricultural low-power and lossy networks (RPAL)," Sensors (Switzerland), vol. 15, no. 8, pp. 19507–19540, 2015.

[78] S. Soursos, I. P. Zarko, P. Zwickl, I. Gojmerac, G. Bianchi, and G. Carrozzo, "Towards the cross-domain interoperability of IoT platforms," EUCNC 2016 - Eur. Conf. Networks Commun., no. June 2019, pp. 398–402, 2016.

[79] I. P. Zarko et al., "Towards an IoT framework for semantic and organizational interoperability," GIoTS 2017 - Glob. Internet Things Summit, Proc., no. June, 2017.

[80] Jell, Thomas, Arne Bröring, and Jelena Mitic. "BIG IoT–interconnecting IoT platforms from different domains." In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 86-88. IEEE, 2017.

[81] L. Hang and D. H. Kim, "Enabling cross-domain IoT interoperability based on open framework," Lect. Notes Electr. Eng., vol. 514, no. December 2018, pp. 687–691, 2019.

[82] Fortino, Giancarlo, et al. "Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach." Integration, interconnection, and interoperability of IoT systems. Springer, Cham, 2018. 199-232.

[83] R. Gravina, M. Manso, A. Liotta, and G. Fortino, Erratum to "Integration, Interconnection, and Interoperability of IoT Systems" (Internet of Things, 10.1007/978-3-319-61300-0), vol. 0, no. 9783319612997. 2018.

[84] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[85] Y. Lee and D. H. Kim, "Threats analysis, requirements and considerations for secure internet of things," Int. J. Smart Home, vol. 9, no. 12, pp. 191–198, 2015.

[86] Gigli, Matthew, and Simon GM Koo. "Internet of things: services and applications categorization." Adv. Internet Things 1, no. 2 (2011): 27-31.

[87] Kamalinejad, Pouya, Chinmaya Mahapatra, Zhengguo Sheng, Shahriar Mirabbasi, Victor CM Leung, and Yong Liang Guan. "Wireless energy harvesting for the Internet of Things." IEEE Communications Magazine 53, no. 6 (2015): 102-108.

[88] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," International Journal of Computer Science and Information Security, vol. 14, p. 456, 2016.

[89] K. A. McKay, K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, Report on lightweight cryptography. US Department of Commerce, National Institute of Standards and Technology, 2017.

[90] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, 2014.

[91] Y. Yu, L. Guo, J. Huang, F. Zhang, and Y. Zong, "A cross-layer security monitoring selection algorithm based on traffic prediction," IEEE Access, vol. 6, pp. 35382–35391, 2018.

[92] Y. Zhang, L. Duan, C. A. Sun, B. Cheng, and J. Chen, "A Cross-Layer Security Solution for Publish/Subscribe-Based IoT Services Communication Infrastructure," Proc. - 2017 IEEE 24th Int. Conf. Web Serv. ICWS 2017, pp. 580–587, 2017.

[93] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," Int. J. Adv. Comput. Res., vol. 9, no. 45, pp. 325–350, 2019.

[94] A. Wang, A. Mohaisen, and S. Chen, "XLF: A cross-layer framework to secure the internet of things (IoT)," Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2019-July, pp. 1830–1839, 2019.

[95] H. Wen, Y. Wang, L. Zhou, X. Zhu, and J. Li, ''Physical layer assist authentication technique for smart meter system,'' IET Commun., vol. 7, no. 3, pp. 189–197, Feb. 2013.

[96] X. Wu, Z. Yan, C. Ling, and X.-G. Xia, ''Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission,'' 2015, arXiv:1502.07565.

[97] H. Park, H. Roh, and W. Lee, ''Tagora: A collision-exploitative RFID authentication protocol based on cross-layer approach,'' IEEE Internet Things J., vol. 7, no. 4, pp. 3571–3585, Apr. 2020.

[98] Y. Lee, J. Yoon, J. Choi, and E. Hwang, "A Novel Cross-Layer Authentication Protocol for the Internet of Things," IEEE Access, vol. 8, pp. 196135–196150, 2020.

[99] S. A. B. Awwad, N. K. Noordin, B. M. Ali, F. Hashim, and N. H. A. Ismail, "6LoWPAN Route-Over with End-to-End Fragmentation and Reassembly Using Cross-Layer Adaptive Backoff Exponent," Wirel. Pers. Commun., vol. 98, no. 1, pp. 1029–1053, 2018.

SURVEY ARTICLE

Authors

Sultana Parween, a Research scholar in the Department of computer science, Jamia Millia Islamia, New Delhi, India. Her area of Research is Computer Networks, Internet of Things, Wireless Sensor Networks, Cloud computing.

Dr. Syed Zeeshan Hussain is currently working as an Associate Professor in the Department of computer science, Jamia Millia Islamia, New Delhi, India. His area of research is Computer Networks, Network Security, and Web Technologies.

Dr. Md Asdaque Hussain received his Ph.D. degree from Inha University, South Korea. He is currently working as an Associate professor & Associate Dean at K L University. His area of research is Computer Networks, Wireless Sensor Networks, and Internet of Things.

How to cite this article:

Sultana Parween, Syed Zeeshan Hussain, Md Asdaque Hussain, "A Survey on Issues and Possible Solutions of Cross-Layer Design in Internet of Things", International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 311-333, 2021, DOI: 10.22247/ijcna/2021/209699.