Solid State Technology
ISSN: 0038-111X
Vol. 63, No. 4, (2020)

A Survey on Routing Protocols With Security in Internet of Things

K. Pradeepa[1], M. Parveen[2]
Cauvery college for women(Autonomous)[Affiliated to Bharathidasan University]
pradeepa.cs@cauverycollege.ac.in; parveen.it@cauverycollege.ac.in

Abstract- The Internet of things (IoT) provides an integration of various sensors and objects that can communicate directly with one another without human intervention. The “things” in the IoT include physical devices, such as sensor devices, which monitor and gather all types of data on machines and human social life. The arrival of the IoT has led to the constant universal association of people, objects, sensors, and services. The main objective of the IoT is to provide network infrastructure with routing protocols and software to allow the connection and incorporation of sensors, personal computers, smart devices, automobiles, and items such as fridge, dishwasher, microwave oven, food, and medicines, anytime and on any network. The development of IoT technology allows numerous IoT devices for various tasks. However, the requirements for the large-scale deployment of the IoT are rapidly increasing, which then results in a significant energy and security concern. This paper provides a standard overview of the routing protocols, security concerns and requirements in the IoT environment. Then, it provides an up-to-date survey of the different IoT routing protocols or algorithms and security schemes.

Keywords- *Routing, Security, Energy Consumption, Large-scale deployment*

I. INTRODUCTION

IoT is an emerging technology used in various applications such as home automation, health care, industries, market, etc. It is attracting considerable attention from both the public and private sectors [1]. An IoT node is a piece of hardware with a sensor that broadcasts data from one place to another over the internet. Types of IoT devices contain software, wireless sensors, computer devices and actuators. Furthermore, they can embed into industrial equipment, mobile devices, medical devices, environmental sensors, and more. Top examples of IoTs are connected appliances, smart home security systems, autonomous farming equipment, wearable health monitors, smart factory equipment, wireless inventory trackers, ultra-high-speed wireless internet, biometric cybersecurity scanners, shipping container and logistics tracking. Fig. 1 shows IoT network architecture. This architecture has a lot of IoT sensors for sensing purpose such as temperature, humidity, pressure etc. After sensing, these data transmitted to a cloud server via IoT gateway. Furthermore, users can access these data through mobile app and so on.

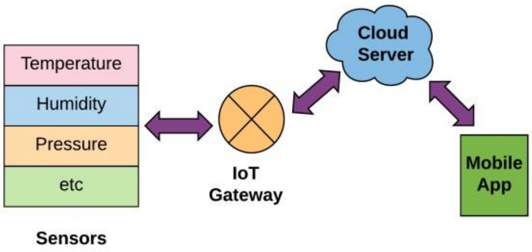


Fig. 1 IoT network architecture

IoT network refers to a smart grid because of the availability of intelligent and low-cost devices, which works autonomously with its sensing, computation and communication capabilities. Also, the proliferation of IoT offers opportunities but may also bear risks. A hitherto neglected aspect is the possible increase in power consumption [2]. IoT devices expected to be reachable by other devices at all times. IoT offers a lot of benefits, among them:

- Scalability: It must have the scalability as it is having any number of devices which are being over the vast network all the machines must identify uniquely. The tags for the devices should give adequately.
- Information and knowledge management: IOT Base station don’t need to give instructions every time to the machine the device is provided with the knowledge and information before it starts functioning and it takes decisions and finds solutions on its own basing on the experience.
- Ubiquitous data exchange: IOT where devices connected through the internet and where the information transferred. IoT has ubiquitous sensors where these are the intelligent sensors gather the information and transfer based on the given input.
- Optimized energy solution: IoT must be able to track even a low powered device, and the consumer must be able to get the most optimal outcome.
- Localization and tracking capabilities: Must be able to track the devices and locate them within a less duration.

- Self–Organization: It is needed to restore the services provided by the devices and to maintain network connectivity. With the advance of internet technology and development of the social network, it is reasonable to expect that a new generation of the internet (also called future internet) that will appear soon. In, several key technical issues [3] of IoT pointed out. These challenges and open problems clarify that the dilemma of current Internet architecture requires significant efforts to change.
- Security: Security providing might be difficult as the automation of the devices has increased, which created new security issues.
- Data management: The communication between the devices completed, every day between the devices lot of data generated. There is a lot of information to be transferred from one place to another. Should check whether the exact data transferred or not. Data management plays a significant role in IOT.
- Storage management: There is a large amount of data generated. When the devices are connected there would be a large amount of data which transferred, they occupy a large amount of data. The other kind is random files where it contains data regarding the devices these files doesn't occupy a vast amount of space. Still, they are large in number they must be accessible very quickly whenever necessary.
- Server technologies: As the number of devices over the network area increases the request, and the number of responses of the device also increases at the same time, it depends on the server. The reaction of the server to the request of the device should complete quickly. There should be no delay in response to the client.
- Insecure authentication/authorization: The administrator will give authentication used to provide permission for the user to access the information and permission used to edit or change the data for that particular application and approval.

A. Characteristics of IoT

The essential characteristics of the IoT are showed in Fig. 2 and discussed as follows [14]:

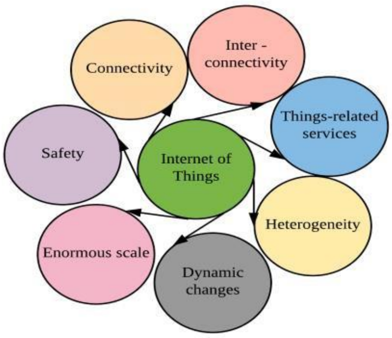


Fig. 2 Characteristics of IoT

- Interconnectivity: With consider to the IoT, anything can link with the global data and communication infrastructure.
- Things-related services: The IoT is able of offering thing-related services within the restrictions of things, for example, confidentiality protection and semantic consistency between physical things and their related virtual things. To give thing- related services within the constraints of things, both the techniques in the physical world and data world will alter.
- Heterogeneity: The nodes in the IoT are heterogeneous as based on various hardware platforms and networks. They can communicate with other devices or service platforms through different networks.
- Dynamic changes: The state of nodes modify dynamically, e.g., sleeping and waking up, disconnected and connected as well as the context of devices includes speed and location. Moreover, the number of nodes can change energetically.
- Enormous scale: The number of nodes is required to manage. These nodes contact with each other will be an order of magnitude better than the devices linked to the internet. Even more critical will be the management of the data created and their interpretation for application reasons. It relates to the semantics of information, as well as proficient information handling.
- Safety: As we achieve advantages from the IoT, we must not forget about security. As both the creators and receivers of the IoT, we must plan for protection. It includes the safety of our private information and the security of our physical well- being. Protect the endpoints, the networks, and the data moving across all of it means making a safety model that will scale.
- Connectivity: It permits network compatibility and accessibility. Accessibility is receiving on a network while compatibility offers the general capability to consume and create information.

IoT generally includes IoT devices with battery power which communicate with each other to transmit a message from a sender device to an IoT Base Station. Due to the Signal Transmission Range Limitation, machines cannot share with others directly. So routing is needed. In IoT, routing means how devices communicate with the base station, transmitting messages that enable them to choose the best paths from the source device to the base station. Furthermore, IoT devices are especially prone to the security threats of eavesdropping, interception, denial-of-service and routing attacks. Some of these problems may solve with the use of cryptographic protocols. In recent literature, many works make specific proposals on how to use well- known cryptographic techniques to secure IoTs. This paper surveys some of the standard and non-standard protocols or algorithms used for network routing and security in IoT network.

II. IOT ROUTING PROTOCOLS / ALGORITHMS

In IoT, nodes are spread in a specific region for a particular purpose and collect the essential data; for example, the data about the temperature, motion, and physical changes. The nodes forward the gathered data to the intermediate nodes due to the restricted transmission range of the node. Therefore, the intermediate nodes use their energy for the packet transmission of the source node, which induces high power consumption of the nodes and thus boosts network partitioning. Therefore, the energy efficiency of the nodes is that the key issue that affects the network performance in distributed networks for IoT. Also, relaying data from a source to a destination is one of the foremost necessary tasks to be carried out on a massive scale and dynamic IoT environment. Therefore, to minimize energy consumption and to enhance the network lifetime, many routing protocols are already designed. This section provides a survey of various existing routing protocols or algorithms.

Cho et al. [4] proposed a Hierarchical Network Architecture based Routing protocol for Energy-Efficient IoT based on Wireless Sensor Networks in Healthcare Environment. To support the energy efficiency of the sensor network constituting the IoT environment, they proposed a subdivided IoT based energy protocol that can dynamically move from one step to another according to the power on/off state of the IoT device. They presented the hierarchical network structure where all objects placed are static and follow the transmission based on static routing (Cluster Heads (CH), Cluster Broker (CB), Relay Node (N-relay), End Node (EN)). The lower layers consist of IoT sensor nodes, cluster heads, relay nodes and cluster coordinators. Next, the topmost layer is the convergence layer. This layer contains base stations—these base stations connected to the internet. In the lower layers, nodes sense the thing or the objects and transmit the data to the N-relay nodes. N-relay passes the data to the CHS. To balance the load on the CHs and cluster broker CBs, CHs pass the data to the upper layer CB which other hands over the data to the upper layer CB and this process continue till the data transmitted to the BS at the topmost layer. They concluded their routing protocol gives balanced energy consumption and better network lifetime.

Silva et al. [5] proposed context-aware routing using fuzzy logic to attain the requirements of specific applications. Fuzzy logic used to translate in math terms the inexact data expressed by linguistic rules set. For this purpose, four Objective Functions (OFs) proposed for the Routing Protocol for Low Power and Loss Networks (RPL). Such OFs are dynamically selected based on context data such as a specific city or regions air quality, remote areas, temperature monitoring and vehicle control flows. The OFs mentioned above created from the fusion of the following metrics: Number of Hops (NH), Expected Transmission Count (ETX) and Energy Consumed (EC). They concluded that their routing increased the lifetime of IoT, to reduce the delay and to improve the reliability and the QoS.

Santiago et al. [6] suggested E2TBR: an Energy Efficient Transmission Based Routing for IoT Networks. A newer node used transmission range or coverage for its parent selection in this process. It means the more current node choose the node which falls at the borderline of the transmission range as its parent. In this way, the number of hops reduced, and the delivery ratio was better. They concluded that E2TBR reduced energy consumption and increased the network lifetime.

Aldabbas [7] proposed Location Prediction Based Routing (LPBR) Protocol for Mobile IoT Systems. He proposed a node rank optimization function based on location predictions along with energy. The LPBR algorithm selected the parent node based on predicted distance from the candidate parent along with remaining energy and resulted in reducing chances of disconnection.

Kaur et al. [8] proposed the Moth Flame Optimization-based Multipath Load Balancing Routing algorithm for IoT applications. This algorithm mitigates the losses of receiving packets from source to the destination and also tries to achieve high packet deliveries for the fewer failures of the node in the Internet of Things (IoT) environment. The Moth Flame Optimization algorithm used to perform optimizations and having less error rate probabilities. Moths fly in the night by keeping a permanent angle concerning the moon, an extremely efficient method for transmitting in a straight line for long distances. They concluded that their routing algorithm achieves fewer loads, less packet loss and high packet deliveries with less energy consumption. Table 1 shows different routing protocols or algorithms comparison.

TABLE 1 DIFFERENT ROUTING PROTOCOLS / ALGORITHMS COMPARISON

Author	**Paper Title**	**Journal Name with Year**	**Protocol / Algorithm**	**Advantages & Disadvantages**
Cho et al. [4]	Energy Efficient IoT based on Wireless Sensor Networks for Healthcare	International Conference on Advanced Communication Technology (ICACT) 2018	Hierarchical Network Architecture based routing	**Advantages:** • Balanced energy consumption • Better network lifetime **Disadvantages:** • Cluster Formation and Route Discovery takes more time. • Packet Transmission Time is high.
Silva et al. [5]	A Proposal for IoT Dynamic Routes Selection Based on Contextual Information	Sensors 2018	Context-aware routing using fuzzy logic	**Advantages:** • Increased the lifetime of IoT • Reduced the delay • Increased reliability and the QoS **Disadvantages:** • This work is not considered a variation in the number of sensor nodes. This work used 20 nodes only within a fixed network topology. While increasing the number of sensor nodes in the IoT network, this work may be a failure.
Santiago et al. [6]	E2TBR: Energy Efficient Transmission Based Routing for IoT Networks	International Journal of Computer Science Engineering and Information Technology (IJCSEIT) 2017	Energy-Efficient Transmission Based Routing (E2TBR)	**Advantages:** • Reduced Hops Count • Reduced energy consumption • Increased network lifetime **Disadvantages:** • Routing overhead occurred during packet transmission in intermediate nodes. • End-to-End delay is high.
Aldabbas [7]	LPBR: Location Prediction Based Routing Protocol for Mobile IoT Systems	International Conference on Future Networks and Distributed Systems (ICFNDS) 2018	Location Prediction Based Routing (LPBR)	**Advantages:** • Reducing the chances of disconnection • High Throughput **Disadvantages:** • This work provides a longer duration of connectivity to the parent node. So the children node lot of times using the same parent node for transmission, the parent node consumes all energy, and it may be dead. So network lifetime is reduced.
Kaur et al. [8]	Improving Multipath Load Balancing Routing With Moth Flame Optimization Approach in Internet of Things Applications	International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) 2018	Moth Flame Optimization-based Multipath Load Balancing Routing	**Advantages:** • Less load • Less packet loss • High packet deliveries • Less energy consumption **Disadvantages:** • While packet travelling in a straight line for long distances, if any interruption occurred, the packet transmission may be a failure. Alternative paths are not considered in this work.

III. SECURITY PROTOCOLS / ALGORITHMS

IoTs have ideal applications in various areas like civilian and military such as surveillance in the battlefield. Different regions and applications of the IoT want safe communications. However, IoTs are prone to different types of malicious attacks, such as impersonating, an interception for misleading because of the connectivity of wireless and the non-availability of physical protection. Thus, it is significant to implement security in IoT is most important. This section provides a survey of various existing security techniques.

Jamshiya et al. [9] proposed a secure Trusted-third-party based key exchange protocol (STKEP) for data communication in the Internet of Things (IOT). They employed an elliptic curve cryptographic method for the encryption process. A session key used to encrypt the data transmitted between the communication parties with the help of a trusted third party. They concluded that STKEP could resist replay, eavesdropping and many other attacks efficiently.

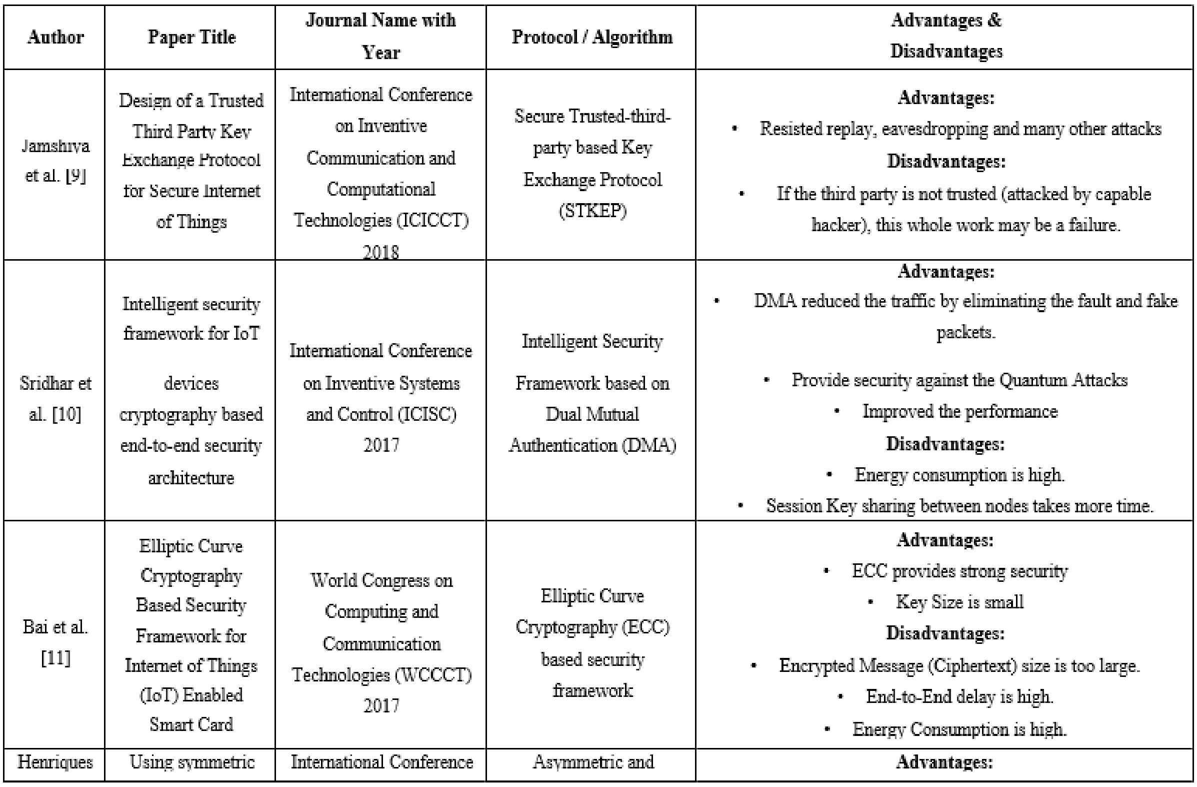
Sridhar et al. [10] proposed an Intelligent Security Framework based on Dual Mutual Authentication (DMA) for IoT Devices. FirstLight Weight Asymmetric Key cryptography used to provide authentication between the sensor node and Device Gateway. The Sensor Node's Unique Id and Device Gateway's unique Id used to create a secret key/Digital certificate using AES Algorithm. Second, the Device Gateway and the Cloud Service mutually authenticated using public Key Encryption-Digital Signature. They concluded that DMA reduced the traffic by eliminating the fault and fake packets.

Bai et al. [11] proposed an Elliptic Curve Cryptography (ECC) based security framework for the Internet of Things (IoT). The ECC based security framework for IoT involves ECC based encryption and decryption and digital signature creation and verification. The message encryption and the authentication ensure unique authentication, integrity, confidentiality and privacy of the information. They concluded that ECC provides robust security for Smart Card implementation.

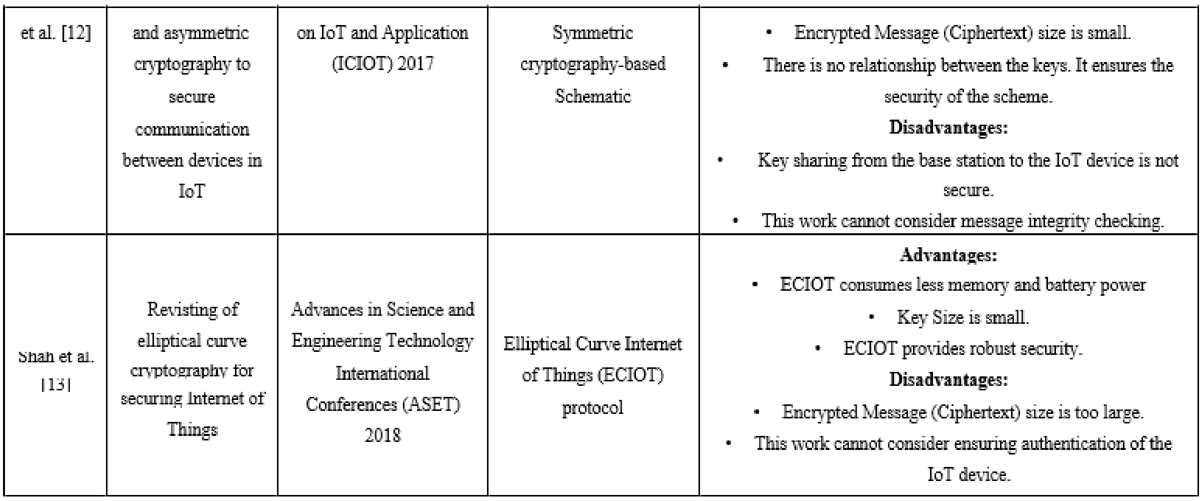
Henriques et al. [12] proposed a schematic consisting of Asymmetric and Symmetric cryptography is defined to secure the communication between the devices in an IoT system. The combination of both Symmetric and Asymmetric cryptography reduced encryption time in preference to merely using an Asymmetric cryptographic algorithm. The use of random keys for Symmetric encryption each time solved the issue of session-key distribution and strengthened the symmetric encryption approach.

Shah et al. [13] proposed the Elliptical Curve Internet of Things (ECIOT) protocol based on the p-192 elliptic curve for key pair establishment in IoT- server communication. The subsequent communication will carry out with symmetric key cipher Ex- OR by using ECIOT derived vital. To optimize the ECIOT protocol projective coordinate system with addition subtraction method for integer recoding has been proposed and utilized. The use of projective coordinates helps protocol to avoid modular inversion operation, which is computationally intensive for 8/16 bit IoT devices. They concluded that the ECIOT protocol consumes less memory and battery power which helps IoT device to have a longer life. Table 2 shows the different security protocols or algorithms comparison.

TABLE 2 DIFFERENT ROUTING PROTOCOLS / ALGORITHMS COMPARISON



Author	Paper Title	Journal Name with Year	Protocol / Algorithm	Advantages & Disadvantages
Jamshiya et al. [9]	Design of a Trusted Third Party Key Exchange Protocol for Secure Internet of Things	International Conference on Inventive Communication and Computational Technologies (ICICCT) 2018	Secure Trusted-third-party based Key Exchange Protocol (STKEP)	**Advantages:** • Resisted replay, eavesdropping and many other attacks **Disadvantages:** • If the third party is not trusted (attacked by capable hacker), this whole work may be a failure.
Sridhar et al. [10]	Intelligent security framework for IoT devices cryptography based end-to-end security architecture	International Conference on Inventive Systems and Control (ICISC) 2017	Intelligent Security Framework based on Dual Mutual Authentication (DMA)	**Advantages:** • DMA reduced the traffic by eliminating the fault and fake packets. • Provide security against the Quantum Attacks • Improved the performance **Disadvantages:** • Energy consumption is high. • Session Key sharing between nodes takes more time.
Bai et al. [11]	Elliptic Curve Cryptography Based Security Framework for Internet of Things (IoT) Enabled Smart Card	World Congress on Computing and Communication Technologies (WCCCT) 2017	Elliptic Curve Cryptography (ECC) based security framework	**Advantages:** • ECC provides strong security • Key Size is small **Disadvantages:** • Encrypted Message (Ciphertext) size is too large. • End-to-End delay is high. • Energy Consumption is high.
Henriques	Using symmetric	International Conference	Asymmetric and	**Advantages:**



et al. [12]	and asymmetric cryptography to secure communication between devices in IoT	on IoT and Application (ICIOT) 2017	Symmetric cryptography-based Schematic	• Encrypted Message (Ciphertext) size is small. • There is no relationship between the keys. It ensures the security of the scheme. **Disadvantages:** • Key sharing from the base station to the IoT device is not secure. • This work cannot consider message integrity checking.
Shah et al. [13]	Revisting of elliptical curve cryptography for securing Internet of Things	Advances in Science and Engineering Technology International Conferences (ASET) 2018	Elliptical Curve Internet of Things (ECIOT) protocol	**Advantages:** • ECIOT consumes less memory and battery power • Key Size is small. • ECIOT provides robust security. **Disadvantages:** • Encrypted Message (Ciphertext) size is too large. • This work cannot consider ensuring authentication of the IoT device.

IV. PARAMETERS AND METRICS FOR EVALUATIONS

Traditional routing and security protocols or algorithms are evaluating the performance according to the following metrics: Throughput, power consumption, End-To-End delay and packet speed.

A. Throughput

Throughput is a measurement of how many units of data can broadcast in a given amount of time. The unit of throughput is kilobits/seconds.

$$TP = TD / TT \quad (1)$$

In equation 1, TP is the Throughput; TD is the broadcasted information between source IoT Device to IoT base station, and TT is Transmission Time.

B. Power Consumption

In IoT, Power Consumption is one of the essential metrics. Each device is receiving and transmitting energy consumption computed. A device which is in sleep mode, it consumes too little energy. The powers for transmission and receiving are fixed values, 0.6 J and 0.4 J, respectively. When a device sends a Packet (P) to the next device, the device's energy capacity will decrease by equation 2.

$$EC = Er + (Dist * PS * Et) \quad (2)$$

EC is the Power Consumption of a device in J; Dist is the distance between a device to the next device in meter, and PS is the Packet Size in Kb. In this way, a device's power consumption calculated.

C. End-To-End Delay

A packet transmission time from a source device to a base station is called End-To-End Delay. From Source to Destination, time taken for a packet to transmit across a network is also called end-to-end delay. It is a one-way delay. It is opposed to Round Trip Time (RTT). In contrast, RTT is a two-way delay.

D. Packet Speed

Packet Speed means a packet takes the distance travelled per unit of time. It is how fast a packet is moving mentioned is equation 3. The unit of Packet Speed is meter/seconds.

$$\text{Packet Speed} = \text{Distance between Source IoT Device to IoT Base Station} / \text{Total Transmission Time} \quad (3)$$

V. CONCLUSIONS

This paper surveys some of the routing protocols or algorithms used for network routing in IoT applications. Five routing protocols or algorithms in IoT studied in this paper. Each routing protocols or algorithm has advantages and disadvantages. But, these existing routing protocols or algorithms common weaknesses are more energy consumption based on high end-to-end delay—a novel minimum energy consumption routing algorithm needed to tackle these disadvantages.

Furthermore, this paper surveys some of the security protocols or algorithms used for network security in IoT applications. Five security protocols or algorithms in IoT studied in this paper. Each security protocols or algorithm has advantages and disadvantages. Common shortcomings of these existing security protocols are key sharing without security, and high energy consumption in terms of high end-to-end delay—secure Key sharing based robust cryptography algorithms with Signature verification technique needed to tackle these disadvantages.

REFERENCES

[1] Ju H, Yoo Y. Efficient packet transmission utilizing vertical handover in the IoT environment. Journal of KIISE. 2015;42(6):807-16.

[2] Shaikh FK, Zeadally S, Exposito E. Enabling technologies for green internet of things. IEEE Systems Journal. 2015 Apr 17;11(2):983-94.

[3] Aijaz A, Aghvami AH. Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective. IEEE Internet of Things Journal. 2015 Jan 12;2(2):103-12.

[4] Cho Y, Kim M, Woo S. Energy-efficient IoT based on wireless sensor networks. In2018 20th International Conference on Advanced Communication Technology (ICACT) 2018 Feb 11 (pp. 294-299). IEEE.

[5] Araújo HD, Rodrigues JJ, Rabelo RD, Sousa ND, Sobral JV. A proposal for IoT dynamic routes selection based on contextual information. Sensors. 2018 Feb;18(2):353.

[6] Santiago. S, Arockiam. L, S. S. A. L. E2TBR: Energy Efficient Transmission Based Routing for IoT Networks. International Journal of Computer Science Engineering and Information Technology Research (IJCSEIT), 2017;7(4), 93–100.

[7] Aldabbas H. LPBR: location prediction based routing protocol for mobile IoT systems. InProceedings of the 2nd International Conference on Future Networks and Distributed Systems 2018 Jun 26 (pp. 1-5).

[8] Kaur S, Rani S, Singh P. Improving Multipath Load Balancing Routing With Moth Flame Optimization Approach in the Internet of Things Applications.

[9] Jamshiya PK, Menon DM. Design of a Trusted Third Party Key Exchange Protocol for Secure Internet of Things (IoT). In2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) 2018 Apr 20 (pp. 1834-1838). IEEE.

[10] Sridhar S, Smys S. Intelligent security framework for iot devices cryptography-based end-to-end security architecture. In2017 International Conference on Inventive Systems and Control (ICISC) 2017 Jan 19 (pp. 1-5). IEEE.

[11] Bai TD, Raj KM, Rabara SA. Elliptic Curve Cryptography based Security Framework for the Internet of Things (IoT) Enabled Smart Card. In2017 World Congress on Computing and Communication Technologies (WCCCT) 2017 Feb 2 (pp. 43-46). IEEE.

[12] Henriques MS, Vernekar NK. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In2017 International Conference on IoT and Application (ICIOT) 2017 May 19 (pp. 1-4). IEEE.

[13] Shah DP, Shah PG. Revisiting of elliptical curve cryptography for securing the Internet of Things (IOT). In2018 Advances in Science and Engineering Technology International Conferences (ASET) 2018 Feb (pp. 1-3). IEEE.

[14] Divyashree, M., & Rangaraju, H. G. Internet of Things (IoT): A Survey. 2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS), 27.

[15] Preethi R, Sughasiny M. PBGTR: PRICE BASED GAME THEORY ROUTING FOR MINIMUM COST ROUTING PATH IN MANET. In2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on 2018 Aug 30 (pp. 469-474). IEEE.

[16] Abd Al-Rahman S, Sagheer A, Dawood O. NVLC: New Variant Lightweight Cryptography Algorithm for the Internet of Things. In2018 1st Annual International Conference on Information and Sciences (AiCIS) 2018 Nov 20 (pp. 176-181). IEEE.

PRADEEPA .K, Associate Professor in Computer Science,CCW,Trichy.

PARVEEN.M, Professor & Head Dept of Information Technology,CCW,Trichy.