

A Reliable Communication Framework and Its Use in Internet of Things (IoT)

Tanweer Alam

Department of Computer Science, Faculty of Computer and Information Systems, Islamic University of Madinah, Saudi Arabia

ABSTRACT

Peoples are naturally communicators but devices are not. In the Internet of Things (IoT) architecture, the smart devices (SDs), sensors, programs and association of smart objects are connected together to transfer information among them. The SD is designed as physical device linked with computing resources that are capable to connect and communicate with another SD through any medium and protocol. The communication among intelligent physical things is a challenging task to exchange information that guaranteed to reach to the destination completely in a real time with the same order as sending without corruption. The reliable communication between physical things can be built in the transmission control protocol (TCP) layers. In TCP layer, the reliable communication is required the error detection, correction and confirmation to exchange information among smart devices. In this paper, the author represents a framework to deal with reliability issues to enable the adoption of IoT devices. The results found the improvement in reliability.

Keywords: Reliability, Wireless Communication, Internet of Things, Transmission control protocol, Sensor Networks.

I. INTRODUCTION

Now the whole world is becoming more and more depending on the mobility services and wireless communication. The drawback of wireless communication is now clear as wireless networking is growing. According to statistica [20] website, by 2020, It is expected that the total number of smart devices connected together will reach up to 50 billion. According to Siemens research, up to 2020, near about 26 billion physical objects will be connected together on the internet (See figure 1). That time is not far away when billions of physical things linked together in real time. They can communicate each other and forwarding and process required data on the cloud. But there is a lack of technical standardization security perspective on the

internet of smart thing. According to Statistica [20] report, in 2025, the total number of connected devices in the world will be approximately 75.44 billion. See figure 1.

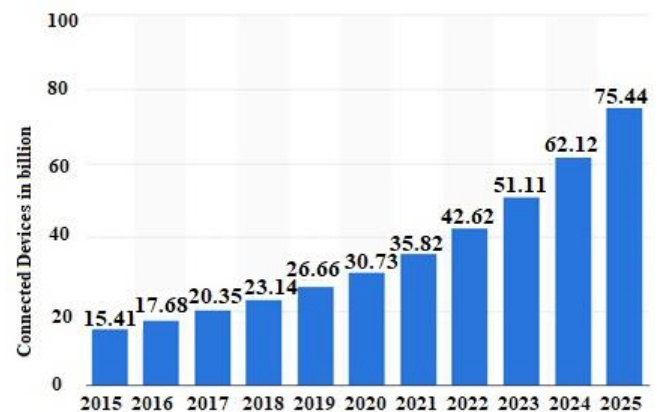


Fig. 1: Internet of Things (IoT) connected devices from 2015 to 2025 (in billions)

The main factor of this growth is not the population of the world but the smart devices. The integrated technologies are playing big role to connect the physical things together and exchange the information among them [11], [12]. This environment where the machine can talk to another machine (Machine-to-machine) and human can talk to machine. The IoT is integration of physical things, smart devices, smart buildings, smart vehicles, embedded objects including electronics, programs, sensors, actuators and network connections to exchange information among each other [13]. The concept of IoT was developed primarily by the wireless sensor network. In 1999, Kevin Ashton presents the idea of internet of things and uniquely identifies physical objects and their location in the internet architecture [14]. The IoT consists of three main components:

- i) Physical Objects
- ii) Sensor Networks
- iii) Data Flow

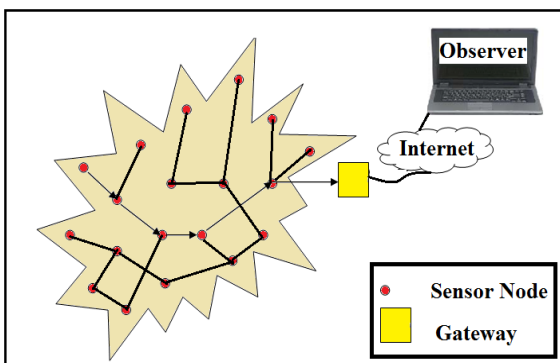


Fig. 2: Observer, Internet and Sensor Nodes

The IoT represents the interconnected physical things that are uniquely identified with sensors [4]. It is the future of communication. The physical object should be smart. It means that the smart object should have unique id, sensor, connection and able to generate events and can be connected to each other. The smart object has the capability to connect in heterogeneous environment [3]. The IoT framework provides the facility to the smart physical things connected each other using standard platform for communication. The development of internet of

physical things is continuously growing with related technologies like cloud computing, sensor network, robotics and Future Internet technologies. The following difficulties are in the development of internet of things.

- i) Difficulties in security and privacy.
- ii) Difficulties in the utilization of uniquely identification.
- iii) Difficulties in large scale testing with complex sensor-based network.
- iv) Difficulties in developing business which embraces the full potential of the Internet of Things.

In this paper, I discussed about the role of reliability in IoT. The IoT is not only one technology but it is a combination of multiple integrated technologies who works together in heterogeneous environment. These integrated technologies are act as an interface between human and machines. After few years, we will see the smart technologies in real word for example cars without drivers, smart factories, smart mines, robots working in organizations. In this situation, the most important thing is reliability in communication between machines. The basic concept of this research is to provide the reliable communication framework between internet of smart devices using IEEE 802.15.4 standard [15]. Many researchers moved in the area of security and reliability in IoT day by day. The reliability can be measured through smart device integrity. The IoT requires an understanding of the connectivity between devices, the development of standards for the transmission of information and tools that enable the autonomous behavior of objects according to the functions to be met and the instructions received from the network that interconnects [16]. Transport and logistics have already long incorporated these technologies, particularly to improve service delivery, and the next evolution is towards the personal and professional environment. The following is the observation that can be happen in next few years.

1. IoT-Cloud: 85-90% IoT data will be stored in Cloud up to 2023.
2. IoT-Security: 85-90% of all information technologies networks will face security problem up to 2020. Hence, they should update their security policy with new IoT policies [17].
3. IoT-Storage: 45-50% IT networks will face the large IoT data handling problem.
4. IoT-embedded infrastructure: 55-60% of IT solutions are becoming integrated by 2018.
5. IoT-smart cities
6. IoT-diversification: after 5 years, all organizations will have their own IoT environments.
7. IoT-Reliability: Most of IoT networks and device need reliable communication.

The reality of interconnectedness things is cooperating man to machines and machine to another machine [1]. They will be talking with each other. But Monitoring and tracking of movable devices are one of the most comprehensive issues. The definition of the internet of things can be described as “a pervasive and ubiquitous system which empowers screening furthermore control of the physical earth by collecting, processing, also analyzing that information created eventually sensors” [9]. The Internet of Things (IoT) is a new approach where several physical things are connected and exchange information among them. The Internet of Things uses Internet in physical things to connect them and exchange information among them. The vision of IoT is the Integration of all physical things with Internet and provide a common platform to connect these physical things anywhere and anytime using the standardization for interoperability. The machine to machine approach [2] might be used for create connection among several devices, these devices can be fixed or moveable. The smart objects (Physical things) is embedded with several technologies like programs, sensors, electronics,

connections and actuators etc. to connect and transfer information to each other. Every connected smart object has unique identification number that is provided by embedded technologies. The smart objects are able to exchange information where they are connected using Internet. The growth of internet of things initially started from 2008 by connecting the physical objects to the internet. The physical objects are connected with a smart database that has a collection of smart data. The framework has the image recognition technology for identifying the physical object, buildings, peoples, logo, location etc. for business and customers. Now internet of things is shifting from information-based technology to operational based technology ie. IPV4 (man 2 machines) to IPV6 (machine 2 machines) [5]. It combines sensors, smart devices and interfaces like Smart Grid. Nowadays increasing numbers of sensors and sensor networks are being connected to the Internet and the World Wide Web. M2M communication is the key technology to support data transfer among sensors. Several tools for turning embedded machine-to-machine communication concepts into working systems exist [6]. In a wider respect, each of the previous consumers has their concerns over cloud computing vulnerabilities and challenges which might prevent them from their objectives.

The following are the components of the internet of things.

- i) Identifiers
- ii) Sensors
- iii) Communications
- iv) Computations
- v) Services
- vi) Semantics

There are three technologies that contributed in the internet of things growths.

- i) The ubiquitous computation that has the capacity of intelligent of physical objects that execute on the computation framework [7].
- ii) Internet Protocol (IPV6) using ubiquitous computing that cover the area of network and support talking of machine to machine. IPv4 internet has a drawback to adding billions of smart gadgets together, but it is possible in IPv6 internet because it enables internet of things to connect billions of smart gadgets together securely.
- iii) Connection using ubiquitous computing that use the fixed cell network or mobility with using sensor connectivity [8].

These technologies should be enhanced regularly so that it allows the progress of internet of smart devices including multi-sensor framework to store, compute, analyze and process capabilities with smaller in size and lowest energies required. The main contribution of this article links a new reliable communication model using IEEE 802.15.4 standard in the area of the internet of things. The communication reliability idea

depends on three main points in the designing of the internet of things architecture.

1. It is not easy to manage information getting from millions of sensors in a centralized framework of smart devices collection.
2. It is not easy to manage network resources in a large network that can collect environment information from the centralized framework.
3. It is very hard to manage sensors that execute the same kind of data parallel and stored on the centralized framework.

II. RELIABLE COMMUNICATION FRAMEWORK

A reliable framework for communication in internet of smart devices has been proposed. According to the article [19], authors considered three ways to handle the reliability issue, firstly one-Transmitter and one-Receiver, secondly two Transmitters and one receiver and finally one transmitter and two receivers [18].

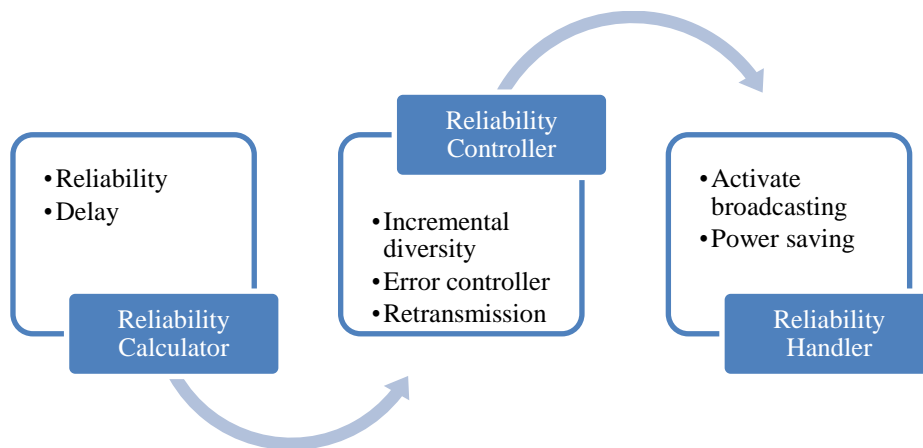


Fig. 3: Reliability Calculator, Controller and Handler

This framework solves the issue of reliability. The IoT devices and sensor network send the utilization streams to the lower layer. The reliability algorithm works in this layer using the power and generate QoS and send it to the upper layer. The control makes the decision and send back to the IoT networks. This process continues until all the data transfer from one smart device to another.

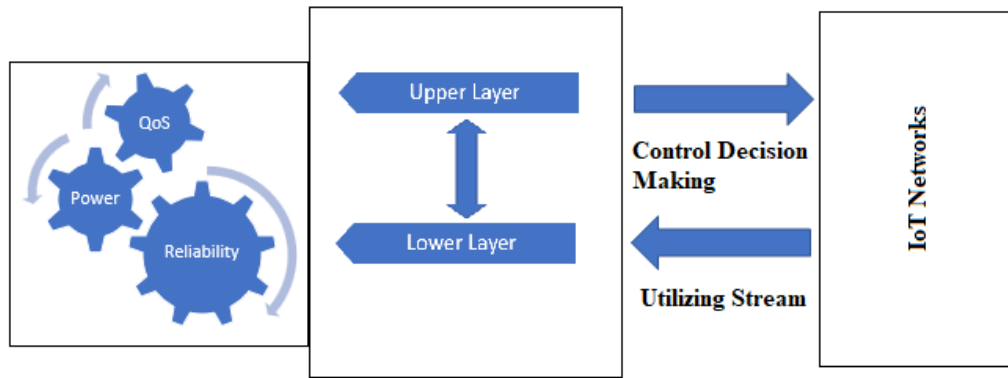


Fig. 4: Reliability framework

The IoT networks may be unreliable in that situation when the networks delayed because of large amount of data need to transmit in a real time. In that situation the delay is referred as failure. In the article [10], the delay function is described as follows.

$$t = t_0[1 + \alpha(r_a)^\beta]$$

Where the t_0 represents the delay, α and β are the parameters, and r_a is the utilization rate. Suppose $t_0=0.023$, $\alpha=25$ and $\beta=7$ then we can calculate the t as follows.

$$t = 0.023[1 + 25(r_a)^7]$$

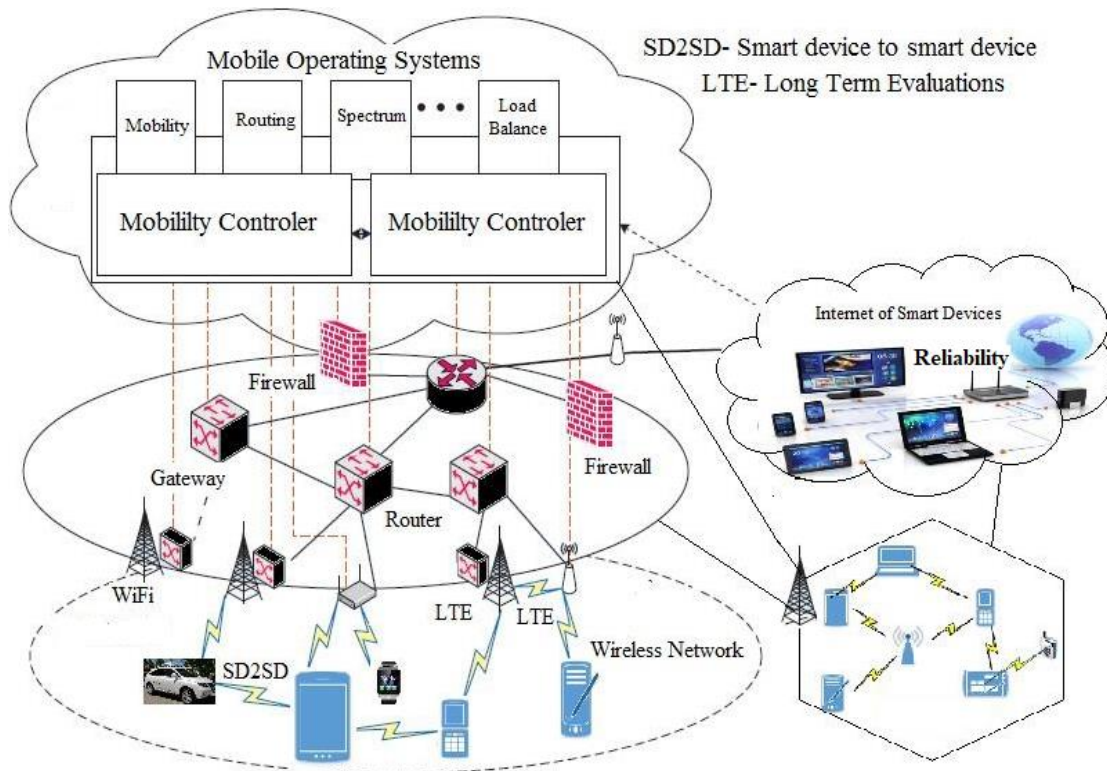


Fig. 5: Reliability in internet of smart devices

The following table represents the reliability of a connection using the path length and the probability of connection failure. Consider the probability of failure is 0.001,0.002,0.003,0.004,0.03 and 0.06. we also consider the length of path is 1,2,3,4.....10.

Table 1: Reliability in IoT when high connection failure probability

P(delay) length	0.001	0.002	0.003	0.004	0.03	0.06
1	0.9990	0.9980	0.9970	0.9960	0.9700	0.9600
2	0.9980	0.9960	0.9940	0.9920	0.9400	0.9000
3	0.9970	0.9940	0.9910	0.9880	0.9100	0.8400
4	0.9960	0.9920	0.9880	0.9840	0.8800	0.7800
5	0.9950	0.9900	0.9850	0.9800	0.8500	0.7200
6	0.9940	0.9880	0.9820	0.9760	0.8200	0.8600
7	0.9930	0.9860	0.9790	0.9720	0.7900	0.8000
8	0.9920	0.9840	0.9760	0.9680	0.7600	0.7400
9	0.9910	0.9820	0.9730	0.9640	0.7300	0.6800
10	0.9900	0.9800	0.9700	0.9600	0.700	0.6200

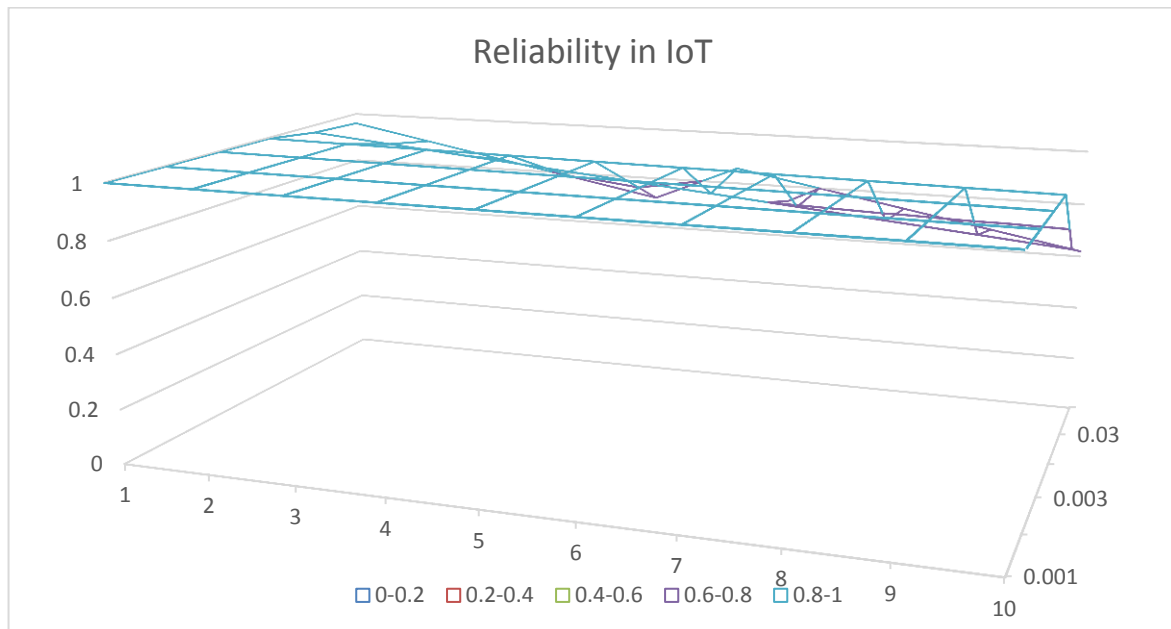


Fig. 6: Reliability in IoT

III. CONCLUSION

In this paper I recognized the reliable communication requirements in IoT. The reliable communication between physical things has been built in the transmission control protocol (TCP) layers. In TCP layer, the reliable communication is required the error detection, correction and confirmation to exchange information among smart devices. In this paper, the author represented a framework to deal with reliability issues to enable the adoption of IoT devices. The results found positive in the improvement of reliability in IOT.

IV. REFERENCES

- [1]. Gummadi, P. Krishna, et al. "Improving the Reliability of Internet Paths with One-hop Source Routing." OSDI. Vol. 4. 2004.
- [2]. Wu, Geng, et al. "M2M: From mobile to embedded internet." IEEE Communications Magazine 49.4 (2011).
- [3]. Li, Xu, et al. "Smart community: an internet of things application." IEEE Communications Magazine 49.11 (2011).
- [4]. Sharma, Abhilash, Tanweer Alam, and Dimpri Srivastava. "Ad Hoc Network Architecture Based on Mobile Ipv6

- Development." *Advances in Computer Vision and Information Technology* (2008): 224.
- [5]. T. Alam and M. Aljohani, "An approach to secure communication in mobile ad-hoc networks of Android devices," 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, 2015, pp. 371-375. doi: 10.1109/ICIIBMS.2015.7439466
- [6]. T. Alam and M. Aljohani, "Design and implementation of an Ad Hoc Network among Android smart devices," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1322-1327. doi: 10.1109/ICGCIoT.2015.7380671
- [7]. M. Aljohani and T. Alam, "An algorithm for accessing traffic database using wireless technologies," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1-4. doi: 10.1109/ICCIC.2015.7435818
- [8]. M. Aljohani and T. Alam, "Design an M-learning framework for smart learning in ad hoc network of Android devices," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1-5. doi: 10.1109/ICCIC.2015.7435817
- [9]. Moslehi, Khosrow, and Ranjit Kumar. "A reliability perspective of the smart grid." *IEEE Transactions on Smart Grid* 1.1 (2010): 57-64.
- [10]. Liu Z, Huang N, Li D. An algorithm for Delay-Reliability in communication networks based on probabilistic user equilibrium model[C]. The 2013 International Conference on Information Science and Cloud Computing (ISCC2013), 2013.
- [11]. Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices." *IJCSNS* 17.5 (2017): 86.
- [12]. Aljohani, Mohammed, and Tanweer Alam. "Real time face detection in ad hoc network of android smart devices." *Advances in Computational Intelligence*. Springer, Singapore, 2017. 245-255.
- [13]. Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." *ARNP Journal of Engineering and Applied Sciences* 12.15 (2017): 4526-4538.
- [14]. Singh, Parbhakar, Parveen Kumar, and Tanweer Alam. "Generating Different Mobility Scenarios in Ad Hoc Networks.", *International Journal of Electronics Communication and Computer Technology*, 4(2), 2014
- [15]. Alam, Tanweer, and B. K. Sharma. "A New Optimistic Mobility Model for Mobile Ad Hoc Networks." *International Journal of Computer Applications* 8.3 (2010): 1-4.
- [16]. Alam, Tanweer, and Tapeshe Kumar Tyagi. "A Random Waypoint Model for Mobility in Ad Hoc Network Simulation Area." *Journal of Advanced Research in Computer Engineering* 3.1 (2009): 13-17.
- [17]. Alam, Tanweer, et al. "Scanning the Node Using Modified Column Mobility Model." *Computer Vision and Information Technology: Advances and Applications* (2010): 455.
- [18]. Bello, Oladayo, and Sherali Zeadally. "Intelligent device-to-device communication in the internet of things." *IEEE Systems Journal* 10.3 (2016): 1172-1182.
- [19]. Mukherjee, Shubhabrata, and Cory Beard. "A framework for ultra-reliable low latency mission-critical communication." *Wireless Telecommunications Symposium (WTS), 2017*. IEEE, 2017.
- [20]. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>