International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 02, July - December 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

Enhancement in Security Frame Work for Bi-Directional Communication with Clock Synchronization in Internet of Things

Satwinder Kaur[1], Amandeep Kaur[2]

Research Scholar, M.Tech (E.C.E Department), DAV University, Jalandhar (Punjab)

Assistant professor, ECE Department, DAV University, Jalandhar (Punjab)

ABSTRACT

The Internet of things is the network in which sense information is passed to the base station (BS) and base station passes the information on the Internet. In the network, multiple levels are involved in the communication due to which chances of security breach is increased.

In this work, the secure authentication protocol is being proposed which is based on secure channel establishment and symmetric key cryptography. The techniques is required which can establish secure channel from source to destination. The technique of time-lay is been proposed which will be synchronizing clock of the nodes and techniques of secure channel establishment provide security of the data.

I. INTRODUCTION

A world-wide system that connects all the computer networks with the help of a standardized Internet Protocol Suite such as TransmissionControl Protocol/ Internet Protocol (TCP/IP) to provide various services to them is known as Internet. “Things” in the IoT sense, can refer to a wide variety of device such as heart monitoring implants biochip transponder on farm animals, electric clams in coastal waters, automobiles with built-in sensor, DNA analysis device for environment/food / pathogen monitoring or field operation device that assist firefight in search and secure operation.

There are millions of users connected across the globe within the private or public sectors, business, government networks or within a local, a global range. The development of Internet has been since the 1970s and has grown around 1980s, where as its usage has mainly grown world-wide within the 1990s. The network interconnection of the regular objects is known as Internet of Things. As there has been an increase in growth of the speed of computations and networking, the Internet of Things have led to a path of smart universe. Internet of Things is a self-configuring type of network which mainly interconnects all the things or objects present within the wireless network. Any item present within the real world that provides communication chain within the regions is known as an entity or object [1].

II. TECHNOLOGIES UTILIZED IN IoT

The various technologies that are involved within the Internet of Things are [2]:

1. *Radio Frequency Identification (RFID)*: RFID uses electromagnetic field to automatically identity and track tags attached to objects. The tags contain electronically stored information. The technology is grouped into

three categories based on the method of power supply provision in Tags: Active RFID, Passive RFID and Semi Passive RFID.

2. *Internet Protocol (IP):* IP the principle communications protocol in the internet protocol suite for relaying datagrams across network boundaries. It's routing function enables internetworking, and essentially establishes the internet. There are five classes of accessible IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while just A, B, and C are regularly utilized [3].
3. *Electronic Product Code (EPC):* EPC is a 64 bit or 98-bit code electronically recorded on a RFID tag and intended to design an improvement in the EPC barcode system. EPC code can store information about the type of EPC, one of a kind serial number of product, its specifications, manufacturer information and so on.
4. *Near Field Communication (NFC):* NFC is arrangement of short-range wireless technology at 13.56 MHz, commonly requiring a distance of 4 cm. NFC technology makes life easier and more convenient for consumers around the globe by making it simpler to make transactions, exchange digital content, and connect electronic gadgets with a touch. It was first developed by Philips and Sony companies. Information exchange rate now days around 424 kbps. Power consumption amid information reading in NFC is under 15ma [4].
5. *Actuators:* An actuator is something that converts energy into motion, which implies actuators drive motions into mechanical systems.Actuators commonly are utilized as a part of manufacturing or industrial applications. Hydraulic and pneumatic systems allow for increased force and torque from littler motor [5].

III. CAPABILITIES OF IoT

From a technical point of view, the Internet of Things is not the aftereffect of a single novel technology; rather, a few complementary technical developments give capabilities that taken together help to cross over any barrier between the virtual and physical world. These capabilities include [6]:

1. *Addressability*: Within an Internet of Things, objects can be located and tended to through discovery, turn upward or name services, and consequently remotely interrogated or configured.
2. *Sensing:* Objects gather information about their surroundings with sensors, record it, forward it or respond directly to it.
3. *Actuation*: Objects contain actuators to manipulate their environment (for instance by converting electrical signals into mechanical movement). Such actuators can be utilized to remotely control real-world processes by means of the Internet [7].
4. *Embedded information processing*: Smart objects include a processor or microcontroller, plus storage limit. These resource scan be utilized, for instance, to handle and interpret sensor information, or to give items a "memory" of how they have been utilized.

IV. APPLICATIONS OF IoT

There are various fields such as the smart homes, forest supervisions and intelligent transport so on in which the IoT has been used now days. There applications have been growing with the increase in the technology. The various fields that utilize the IoT are described briefly below [8]:

1. *Smart Home*: In this filed the main function is to handle the monitoring of home environment and managing the electrical equipment's present within the specific areas. There are various components present within such applications which mainly comprise of electrical equipment, agent devices and many other devices. The main object here is to transmit the data, provide access authentication, provide agent management and monitor the surrounding environment.
2. *Forestry Monitoring*: The management of the forest resources is done here along with the examination of its surrounding environments. There is an IoT forest environmental factors collection platform present within the Internet of Things which is based on the ZigBee. It helps in measuring the surrounding environment components such as temperature, humidity, light intensity etc.
3. *Intelligent transportation*: Within this application, the traffic conditions are monitored here and important information regarding them is conveyed to other resources. On the basis of the information shared across the vehicles, the drivers benefit by avoiding accidents to occur and drive safely. There are roadside detection units, on-board units, backend server as well as client terminals present within this complete system. The cameras are utilized for gathering the information related to the traveling details, road conditions and other environmental conditions present in the particular scenario [9].

V. PROPERTIES OF IoT

There are various objects present within the IoT systems which are different from each other with respect to their sizes and types. Also, their features and access capabilities are different from each other. The broader aspects in which the properties of the objects can be stated are thus identified. The resource granularity, functional characteristics as well as the access capabilities are the three important aspects which are explained below:

1. *Resource Granularity:* With respect to the size of the resources, the objects can be categorized into coarse and fine resources in IoT systems. On the basis of the complexity of the structure and the function the granularity of the resources can be distinguished. There are various components such as sensors, controllers and RFID equipment which can provide the information regarding the type of resource present. [10].
2. *Functional Characteristics:* The classification of objects within the IoT on the basis of the functions can be done into the single functions as well as complex function systems. Only one sort of basic function is provided by the single-function devices within the IoT. For example, there are innumerous sensors present within the applications which help in providing information regarding the environment surrounding them. There are also various controller devices present within the home appliances mostly which help in managing the environment of the home or the machines present within the industries.
3. *Access Capabilities*: There are equipment's and resources present within the objects which can access the IoT and provide wide range of information. There are various components or objects present within the IoT infrastructure. For example, in the case of telephones or smartphones, there are various components present in the hardware as well as software aspects which help in establishing the communication amongst various devices. Same is the case seen in computers or laptops. There are various industrial devices as well which comprise of various objects which are based on the M2M technology. All these examples provided above use the applications of IoT in one way or the other [11].

VI. ACCESS REQUIREMENTS OF IoT

There are various devices that are not provided access within the Internet of Things systems as they have a lot of information available within them and are present within the real world. These access requirements are to be analyzed within the IoT devices. They are explained below:

1. *Functional Requirements*: There should be a correct identification and certification of the access devices present within the Internet of Things. For instance, the unique MAC or IP addresses of the computers can be utilized for identification when it tries to access the internet. There is need of external hardware as well as software resources for executing their own specific perception, control or computing functions with the help of the access restricted devices present within the IoT systems. For providing intelligence control for example, within an industry, the controller needs to receive the control direction from the higher platforms.
2. *Non-functional Requirements*: For the need of performing better, the hardware and software resources are expanded by the access restricted devices in the case of non-functional requirements. With respect to the hardware resources there are some restrictions made on the access restricted devices. For example, the calculation and storage performance of the networks is very less in case of few sensor networks. There is no communication performed by a few industrial controllers. There is a need of coordination among various software and hardware resources as the hardware performance of such industrial controllers cannot undergo normal implementation of the respective functions. [12].

VII. TECHNOLOGICAL CHALLENGES OF IoT

While the possible applications and scenarios laid out above might be extremely interesting, the demands put on the underlying technology are substantial. Progressing from the Internet of computers to the remote and to some degree fuzzy goal of an Internet of Things is something that must in this manner be done slowly and carefully, for example:

1. *Scalability*: An Internet of Things potentially has a larger general degree than the conventional Internet of computers. In any case, on the other hand, things cooperate for the most part inside a local environment. Essential functionality, for example, communication and service disclosure in this manner need to function similarly efficiently in both small-scale and large-scale environments.
2. *Arrive and Operate*: Smart regular objects might not be perceived as computers that require their clients to configure and adapt them to specific situations. Mobile things, which are regularly just sporadically utilized, need to build up connections suddenly, and organize and configure themselves to suit their specific environment [13].
3. *Data Interpretation*: To support the clients of smart things, we would need to decipher the local setting dictated by sensors as precisely as could be expected under the circumstances. For service suppliers to profit from the disparate data that will be created, one should have the capacity to draw some generalizable conclusions from the interpreted sensor data. Be that as it may, producing helpful information from raw sensor data that can trigger further action is in no way, shape or form a trivial undertaking [14].

VIII. SECURITY IN IoT

There is a lot of research being proposed related to the security of IoT devices. However, not much focus is given towards the interaction of IoT devices with their respective owners. An integral part within the IoT systems is to control and manage them remotely. There must be however, a precise handling of the access provided to them. There are various critical tasks for instance, that can be handled by the IoT devices present within the mechanical control applications such as controlling the temperature of fridges, handling the air toxic gases and quality of air and many more [15]. There are a lot of security issues arising within the IoT device which are mainly to the internet framework utilized. Basically, the collection of physical object across the internet is known as Internet of Things. Thus, various security issues might arise within them. Some of them explained below [16]

1. Security issues in Perception Layer

The lowest level of the Internet of Things deployment in the perception layer which is mainly a source through which the information can be accessed within the complete IoT devices. The physical securities of the sensing devices are involved within the perception layer along with the information gathered by it. There is a no guarantee of the security provided by the framework within Internet of Things. Due to the diversity, limitation of energy, and the poor preventive mechanisms there are more chances of attacks within the IoT systems. This affects the security of the sensing nodes that are present within the applications that involve WSN, RFID, and M2M terminal within them. The perception layer the various issues involved have made it prone to attacks that are not easy to be prevented.

1.1 ***Security issues in the Wireless Sensor Networks (WSNs):*** The network within which numerous nodes are present for sensing and managing the environment surrounding them is known as wireless sensor networks. There is a proper connection established within the humans or computers and the environment surrounding the network for providing an ease of interaction. There are various components that comprise within a wireless sensor network such as the sensor nodes, actuator nodes and so on [17].

1.2 ***Security issues in Radio Frequency Identification Technology in Internet Things*****:** There are various RFID tags which are utilized for automatic the exchange of information within the RFID systems. There is a large vulnerability of the RFID tags towards the external attacks. This is due to the poor security status of these systems [18]. There are various attack which can occur here. Some of them are enlisted below.

1.2.1 ***Unauthorized tag tracking*****:** The tags can be tracked by the malicious users and thus the sensitive information can no longer be safe and can be outsourced to unauthorized users. In such cases, the clients that are about to buy any product which has an RFID tag guarantee will provide no confidentiality and the privacy will be depleted. So, it is a loss for the application as well as the customer.

1.2.2 ***Replay Attacks*****:** A response from the tag is used by the attacker here within the replay attacks. The attacker impersonates the tag and sends it to the unauthorized user [19]. There is an interception in the communication signal between the reader and the tag within these types of attacks.

2. SECURITY ISSUES IN PHYSICAL LAYER

The various functionalities such as the encryption, decryption, demodulation, transmission, collection of information and so on are performed within the physical layer. There are various types of attacks possible within this layer. Some of them are:

1. *Selective Forwarding*: Within this type of attack, numbers of selective nodes are only forwarded by the compromised node and the considerable numbers of nodes are not forwarded completely. The malicious objective of the attacker is achieved by determining the number of nodes as per its requirements. These nodes are not able to forward the packets of information further along these paths [20].
2. *Sybil*: A single node is replicated by the attacker and multiple identities are provided for alternating the nodes within this attack.
3. *Wormhole*: The relocation of bits of information is done within the wormhole attack and these bits are moved from their original unique positions. The bits of information are passed across a connection which has low latency for relocating the data packet.

3. SECURITY ISSUES IN APPLICATION LAYER

The communication technology, computer technology and industry professionals when integrated together can be equalized to the affects that are generated by the individual IoT technique. Various numbers of viewpoints can be identified by the applications of IoT within various fields. There is various security issues found within the application layer. Eavesdropping and tampering are two of such attacks. The management of traffic can be done in a proper manner through this layer [21]

IX. RESEARCH METHODOLOGY

Firstly, we deploy the network with infinite sensor nodes. All the sensor nodes are grouped into clusters. According to the sensor nodes these clusters are formed. Each cluster has a cluster head. Cluster heads are chooses by election algorithm. A node in a cluster which has more resources and energy is selected for cluster head. All the nodes forward their data to cluster heads and cluster heads forward the data to their respective destinations. For transmission, route is discovered by AODV routing protocol. The path is established between source and destination. AODV routing protocol discover the virtual paths means dynamic paths. After the path discovered the transmission take place. All the sensor nodes should be synchronized with cluster head to avoid the packet collision. There is a sink available at the network. After that, there are clusters having cluster head and node in it. First of all, one cluster head will send message to the sink. After receiving message sink will minus cluster head will set its clock according to the current timing after reducing delay. This process will continue until all the cluster head gets the similar clock. Same process will be applicable to the clock synchronization between cluster head and node in a cluster.

X. EXPERIMENTAL RESULTS

1. Throughput Comparison

As shown in the figure below the throughput of the proposed and existing scenarios are compared and it is being analyzed that network throughput is increases at steady rate after clock synchronization. Throughput comparison of existing and proposed techniques as shown in figure 1.

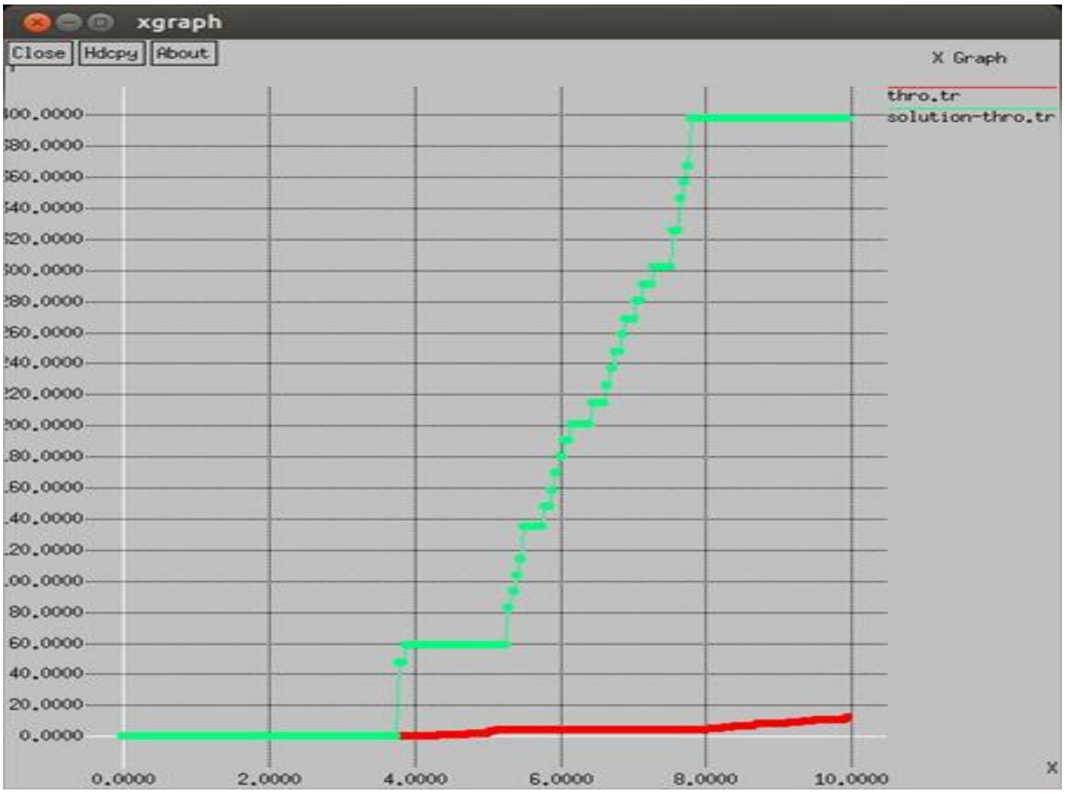

Figure. 1: Throughput Comparison

Table 4.4*: Throughput Comparison*

Time(sec)	Existing technique	Proposed technique
0	2.00	4.00
2	3.00	10.00
4	5.00	60.00
6	8.00	200.00
8	11.00	400.00

2. Packet loss Comparison

The packet loss of the proposed and existing techniques is compared and it is being analyzed that when the clocks of the sensor nodes get synchronized packet loss is reduced which increase network efficiency. Packet loss comparison of existing and proposed techniques as shown in figure 2.

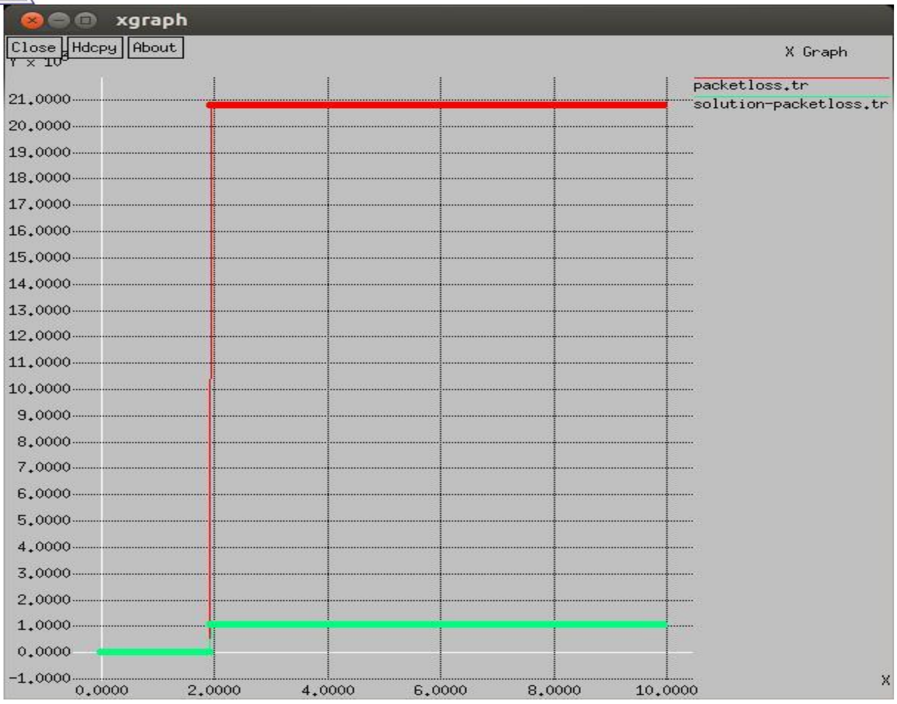

Figure. 2: Packet loss Comparison

Table 4.3: Packet loss Comparison

Time(sec)	Existing technique (no. of packet)	Proposed technique (no. of packet)
0	0.00	0.00
2	1.00	1.00
4	21.00	1.00
6	21.00	1.00
8	21.00	1.00
10	21.00	1.00

3. Energy Comparison

The energy of the network is consumed when any packets send or received in the network. In the existing scenario, the packet loss in the network is high which increase energy consumption. In the proposed technique when clocks get synchronized energy consumption is reduced. Energy comparison of existing and proposed techniques as shown in figure 3.

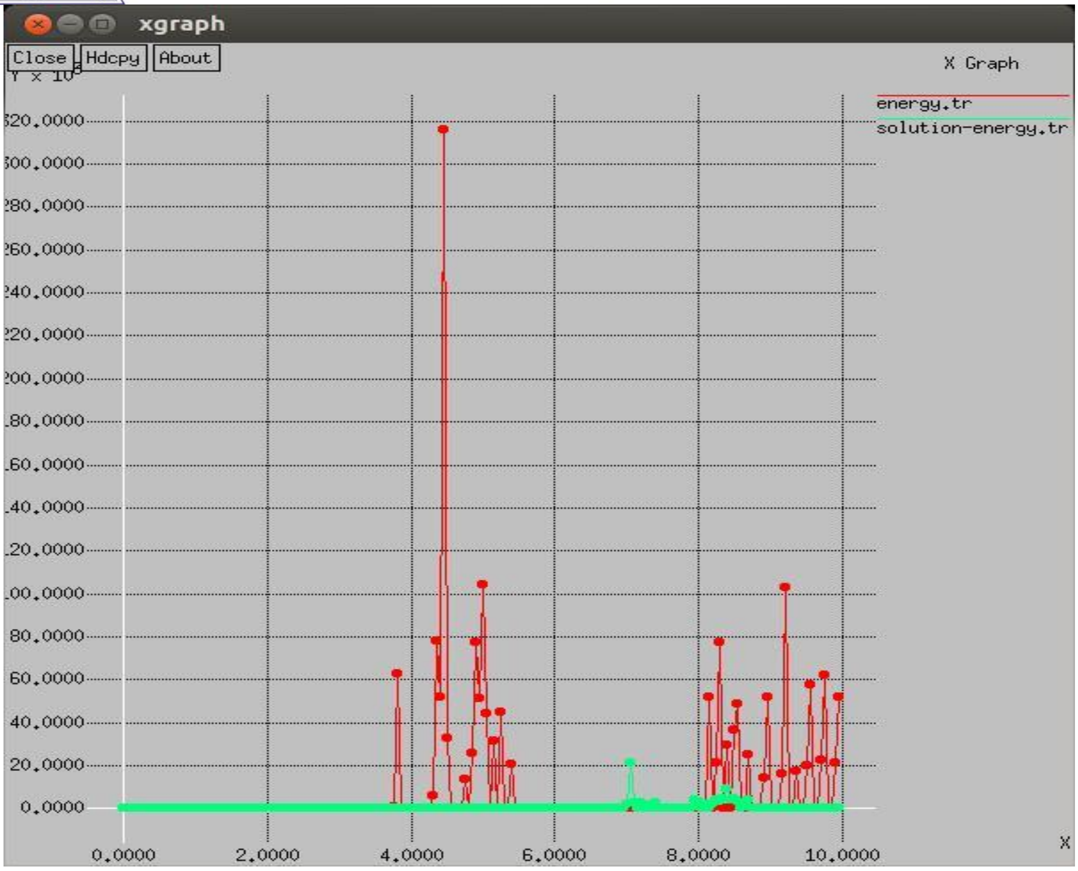

Figure. 3 Energy Comparison

Table 4.2: Energy comparison

Time(sec)	Existing technique (joule)	Proposed technique (joule)
0	2.00	4.00
2	4.00	2.00
4	60.00	5.00
6	5.00	3.00
8	70.00	10.00
10	80.00	7.00

4. Delay Comparison

The existing and proposed scenarios are implemented and it is being analyzed that delay of the proposed technique is reduced as compared to existing due to clock synchronization in the network. Delay comparison of existing and proposed techniques as shown in figure 4.

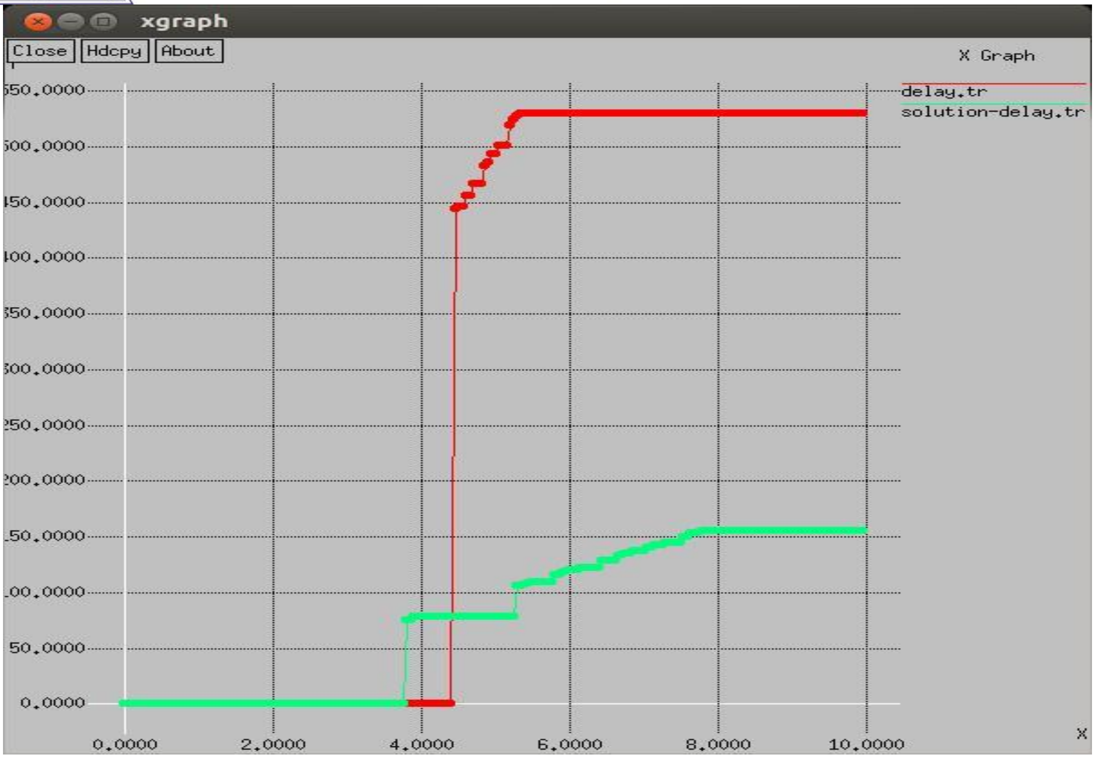

Figure. 4 Delay Comparison

Table 4.1: Delay Comparison

Time(sec)	Existing technique	Proposed technique
0	3.00	2.00
2	2.00	5.00
4	5.00	75.00
6	525.00	125.00
8	525.00	150.00
10	525.00	150.00

XI. CONCLUSION

IoT is a broad term alluding to applications such as Internet-connected vehicles, consumer gadgets and smart phones. In any case, the edge of the IoT network will consist of simple sensors and wireless devices that give, in addition to other things, the identification of objects, sensing, control and automation. In this work, the technique which is being proposed, based on generating symmetric key for secure generation of data between source to destination. To encrypt and decrypt the data symmetric encryption algorithm is used and key which is used for encryption and decryption is renewed time to time. Secure channel establishment protocol is used for symmetric key generation and secure channel protocol also maintain clock synchronization. NTP protocol is not used rather GPS system is used for clock synchronization and for network bandwidth consumption. The time lay technique is applied which synchronize the clocks of the devices. The RSA algorithm is applied which establish secure channel from source to destination. The simulation is being performed in NS2 and it is being analyzed that proposed technique performs well in terms of throughput, energy and delay.

REFERENCES

[1] Chinmaya Mahapatra, Zhengguo Sheng and Victor C.M. Leung," *Energy-efficient and Distributed Data-aware Clustering Protocol for the Internet-of-Things",* 2016, IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 978-1-4673-8721-7

[2] J. Yun, Il-Y. Ahn, N.-M. Sung, and J. Kim, "*A Device Software Platform for Consumer Electronics Based on the Internet of Things"*, 2015, IEEE Transactions on Consumer Electronics, Vol. 61, No. 4

[3] L. Atzori, A. Iera, and G. Morabito, "*The Internet of Things: A survey*", Computer Networks, Vol.54, 2010, p. 2787-2805

[4] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen," *Capillary Networks – Bridging the Cellular and IoT Worlds,"* 2015, IEEE 2nd World Forum on Internet of Things

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "*Internet of Things (IoT): A vision, architectural elements and future direction",* 2013, Future Generation Computer Systems, Vol.29, p. 1645-1660

[6] H. Suo, J. Wan, C. Zou, and J. Liu, "*Security in the Internet of Things: A Review,"* 2012, in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, no., pp. 648-651

[7] J. Granjal, E. Monteiro, and J. S´a Silva, *"Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,*" 2015, IEEE Communications Surveys & Tutorials Volume: 17, Issue: 3, pp. 1294-1312

[8] R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, and D. Valletta, *"Security implementation in heterogeneous networks with long delay channel,"* 2012, IEEE 1st AESS European Conference on Satellite Telecommunications, ESTEL 2012, Rome, Italy, p.1-5

[9] 1.S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, *"Security, privacy and trust in Internet of Things: The road ahead,"* 2015, Computer Networks, Volume 76, 15 Pages 146-164

[10] R. H. Weber, *"Internet of Things – New security and privacy challenges,"* 2010, Computer Law & Security Review, Vol. 26, No. 1, pp. 23-30

[11] Buragohain, C.; Agrawal, D.; Suri, S., "*Power Aware Routing for Sensor Databases*", 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005), Miami, FL, USA, pp.1747–1757

[12] Singh, S.; Woo, M.; Raghavendra, C.S., *"Power-Aware Routing in Mobile adhoc Networks",* 1998, 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), New York, USA, pp.181–190

[13] Stojmenovic, I.; Lin, X., *"Power aware localized routing in wireless networks*", 2001, IEEE Trans. Parall. Distr. 12, 1122–1133

[14] Li, N.; Hou, J.C., *"Topology Control in Heterogeneous Wireless Networks: Problems and Solutions",* 2004, 23th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004), Hong Kong, pp. 1735–1746

[15] A. K. Sadek, W. Su, and K. J. R. Liu "*Multimode cooperative communications in wireless networks,"* 2007, IEEE Trans. Signal Processing, vol. 55, no. 1, pp. 341-355

[16] R. Zhang, M. Wang, X. Shen, "*Probabilistic analysis on Dos provisioning for Internet of Things in lte-a heterogeneous networks with partial spectrum usage,"* 2016, IEEE Internet of Things Journal, vol. 3, no. 3, pp. 354-365

[17] J. Feng, Z. Feng, Z. Wei, W. Li, and S. Roy, "*Optimal base station density in ultra-densification heterogeneous network,"* 2015, IEEE Wireless Communications and Networking Conference (WCNC), pp. 1452-1457

[18] J. Granjal, E. Monteiro, and J. S. Silva, "*Security for the Internet of Things: A survey of existing protocols and open research issues,"* 2015, IEEE Communication. Survey Tuts., vol. 17, no. 3, pp. 1294–1312

[19] Q. Xu, P. Ren, H. Song, and Q. Du, "*Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations,"* 2016, IEEE Access, vol. 4, pp. 2840-2853

[20] H. Wang, T. Zheng, and X. Xia, "*Secure miso wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading,*" 2015, IEEE Transactions on Wireless Communications, vol. 14, no. 1, pp. 94-106

[21] H. Wang, and X. Xia, "*Enhancing wireless secrecy via cooperation: signal design and optimization,"* 2015, IEEE Communications Magazine, vol. 53, no. 12, pp. 47-53