IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

A Secure and Efficient Clock Synchronization Technique in IOT Using Time Lay and RSA

Jaskaran Singh Gill[1], Harpreet Kaur[2]

Department of Computer Science and Engineering, Lala Lajpat Rai Institute of Engineering and Technology, Moga, Punjab[1,2]

Abstract: The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enable these things to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions. In the proposed work, by-hop encryption technique is utilized within the traditional network layer in order to encrypt the information within the transmission process. However, with the help of decryption and encryption operations, there is a need to keep plain text within each node. There is end-to-end encryption mechanism applied within the traditional application layer. This means that for sender as well as receiver, the information is only kept explicit. There will always be encrypted information provided within the transmission process as well as during the forwarding of nodes. There is a need to select amongst by-hop and end-to-end encryption within IoT systems since network layer and application layer are connected so closely. Only the links that require protection can be encrypted in case when by-hop encryption is adopted. This is due to the reason that various applications can be implemented safely when this approach is applied to all business within the network layer. Thus, there is transparency of security mechanisms to business applications with the help of which it becomes convenient for end users to access services. The clocks of the IoT devices are not well synchronized due to which security of the network gets compromised. The work synchronizes clocks of the IoT devices and also establish secure channel from source to destination for data transmission. The work has been evaluated using various performance metrics; energy, throughput, packet loss and number of dead nodes. The proposed work leads to increased security of the network and reduced packet loss in the network.

Keywords: RSA, Time lay, clock synchronization, IOT, Security

I. INTRODUCTION

A worldwide system that connects all the computer networks with the help of a standardized Internet Protocol Suite (TCP/IP) to provide various services to them is known as Internet. There are millions of users connected across the globe within the private or public sectors, business or government networks or within a local or a global range. The network interconnection of the regular objects is known as IOT. As there has been an increase in growth of the speed of computations and networking, the IOT has led to a path of smart universe [1]. IOT 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. The communication possibilities that can help in providing data transmission within certain paths with the help of various objects are the main goal of the IOT systems. RFID (Radio Frequency Identification) is the main goal of the IOT systems. A global infrastructure can be built for RFID tags within the IOT which can mainly be performed with the help of a wireless layer present on the top of the Internet providing the services [2]. On the basis of the properties like identification, confidentiality, integrity, as well as undeniability, the security of data as well as network should be provided. Within various crucial areas related to national economy, there are several IOT applications introduced apart from internet. The applications such as medical service, health care as well as intelligent transportation are mostly found today [3]. Thus, there is need to provide higher availability as well as dependability within the IOT systems in order to provide efficient outcomes. The internet is extended to physical world with the help of IOT technology due to which various security and privacy issues have risen. The internal properties of IOT as well as the differences of this technology against other traditional networks are mainly the reasons of causing such issues. In order to attack the IOT systems, several adversaries have come up. The examination of various security issues as per the information flows and potential adversarial points of control is very important in order to protect the system from various attacks [4]. A defense in-depth of system cannot be achieved by putting together the security mechanism of each logical layer due to which the IOT system remains stable-persisting for whole time duration. Thus, in order to create security structure through the combination of control and information, solutions are to be provided. In order to provide enhanced security mechanism, key management is an important step. Within the cryptographic security, key management is the most difficult part.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

There have been no ideal solutions found yet by the researchers. There is no involvement of lightweight cryptographic algorithm or higher performance sensor node. Often there is application of real large-scale sensor network. The important parts of research will thus be the various issues that have been arising related to network security in various scenarios [5]. The major focus is still not completely upon the security law and regulations. Also, within IOT there is no technology standard provided as well. In relevance to national security information, business secrets as well as personal privacy, the IOT systems are generated. Thus, in order to promote development of secure IOT systems, proper legislative points need to be covered. The IOT systems are developing largely within various applications along with the development of radio frequency identification (RFID), pervasive computing technology, network communication technology and various other systems. In order to ensure better performance of systems, higher security is required. There are many severe security challenges being faced within IOT as well. An appropriate security structure needs to be built here [6]. In Diffie-Hellman Algorithm for Security Access Protocol the two types of communication are possible between the gateways and the mobile devices. The data from the mobile devices is transmitted to the gateway which is transmitted to the IP-based backbone. The IP-based backbone will transmit data to service platforms. The Diffie-Hellman algorithm is applied to establish secure channel between the mobile devices and gateways for the bidirectional communication. In the communication, mobile device will select one public key and also select private key which is permitted root of public key. The gateway will also select one public key and also make private key which is primitive root of public key [7]. The secure channel is established between the both parties when they agreed on the common key "k". The data from the mobile device will be transmitted to the gateway through the established secure channel.

II. LITERATURE REVIEW

Z. Guo et.al (2016) proposed that the communication between the end points of devices with the help of physical objects present over the internet known as Internet of Things. The IOT services have known to provide ease in our day to day lives. But the systems have various vulnerabilities as well which might result in causing various issues related to the systems. There is a need of proposed examination of the systems from the very small level present within them [9]. The merits and demerits related to the biometric within the IOT systems are also described. There are various issues such as reverse engineering, tampering and unauthorized access within the IOT systems that are to be prevented with the help of various new biometrics merged within the previous ones. It is seen through the results achieved that the enhancement made has been beneficial.

M. Mohsin et.al (2016) proposed an ontology-based framework for the IOT for providing security to these systems. There are various APTs (Advanced Persistent Threats) that occur within the systems and can be prevented with the help of certain measures. There are specific tasks that were performed here [11]. There are various already existing ontologies within the CTI (Cyber Threat Intelligence) standards which needed to be examined here. The comparisons of these already stated mechanisms are done with the new concepts and the novel IOT ontology is proposed. From the XML-based threat feeds, the related information is extracted by the framework. The simulation results achieved here showed the improvements that have been mainly seen with the help of new changes made.

R. Kodali et.al (2016) presented that there were various remote interfacing and monitoring issues that aroused when a device was connected with the Internet in the case of IOT. This method could similarly be applied in the home automation systems with the help of various sets of sensors in the systems which notified the important things and helped the actions to be controlled as per required [12]. As per the experimental results it could be seen that various enhancements when made within the systems, the applications could be made to run as per the needs of the users. Such enhancements are very useful and could be utilized in a huge number of applications mainly within the home automation systems.

V. Kharchenko et.al (2016) presented that the SBC (Smart Business Center) system was one of the most important subsystems within the IOT systems related to their security when the complexity was higher. The various issues arising in the design and operation of SBC systems are discussed in this paper. The reliability and security of the system at various instants is to be done by examining their safety. The SBC is designed in such a manner that the hardware and software mechanisms are seen by the manufacturers in a proper manner [13]. It is also important to ensure the security of SBC routers which could be done with the help of introducing various measures in it. The vulnerabilities detected within the system had resulted in exposing the system to hacker attacks which could destroy the privacy of the complete system.

P. Wortman et.al (2017) stated that the IOT devices are widely being used in the medical and healthcare domains. In this research the issue of poor security designs and implementation in medical IOT devices was addressed by proposing the utilization of existing modeling software AADL (Architecture and Design Language) as a method of institutionalization of medical IOT device development [8]. Generally speaking, the method would eventually need to

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

measure the performance of these large IOT networks, however it is find that the result is totally different without some planning from a development stance. Consequently this work proposed utilizing the powerful and flexible modeling language AADL to account for constraints and different concerns of over-engineering IOT devices inside the healthcare domain.

T. Abels et.al (2017) IETF impressively defined Internet interoperation crosswise over 30 years of unforeseeable punctuation API. IOT needs comparative future confirmation, however for associated things' compos able semantics, security, reliability and QOS (Quality of Service). This research reviewed these with streamlining tradeoffs from a bottom up approach utilizing DDS (Data Distribution Service). At that point abnormal state semantic augmentations to DDS are suggested for semantics that were backward compatible, while keeping up the security, reliability and QOS of DDS [10]. This author presents a SSN (Social Security Number) framework that consolidates the semantic endpoints of information centric with strong semantics, supporting resource discovery for semantic sensor and event annotations. This initiates compos able semantics, while extensions remained DDS compatible for proceeding with information security, QOS and reliability.

III. RESEARCH METHODOLOGY

This work is based on clock synchronization and secure channel establishment for communication in IOT. To introduce the clock synchronization, the technique of time lay will be used in which base station of each cluster of nodes will share its clock time with internal nodes of its own cluster, they in return share their clock time with base station. Base station will then calculate the average clock time. Similarly the other clusters of that network calculate their average clock time. After this all clusters will share their calculated clock times with each other and finally the clock of all clusters is set according to this new calculated average. In this way it will provide efficient clock synchronization. The secure channel establishment technique will be applied for both uni-directional and bi-directional communication. The technique of RSA algorithm will be applied which establish secure channel from source to destination. This leads to increased security of the network. Also, asymmetric keys will be exchanged through the secure channel.

3.1 RSA Algorithm: An asymmetric encryption algorithm proposed in 1978 which was mostly accepted and implemented within public applications is known as the RSA algorithm. This type of algorithm can be utilized for both data encryption as well as digital signature. On the basis of large integers as well as prime testing, this algorithm is proposed.

Advantages:

- The RSA algorithm uses the symmetric cryptosystem which is fast and efficient as compared to asymmetric cryptosystems.
- The algorithm is secure because no keys are transmitted from the channel which reduces the chances of man-in-middle attack.

Disadvantages:

- The unauthorized user can publish the fake public-key which leads to wrong generation of shared key. Due to wrong generation of the shared key, source and destination are unable to communicate with each other.
- The RSA algorithm is based on prime numbers for the secret key generation. The efficiency of prime number generation is quite low which makes it difficult to achieve complex secret key.
- The generation of secret key needs lots of calculations and inputs. This results in slowing down the speed of RSA algorithm.

3.2 Time Lay Technique: Time Synchronization in wireless networks is extremely important for basic communication, but it also provides the ability to detect movement, location, and proximity. The synchronization problem consists of four parts: send time, access time, propagation time, and receive time.

3.2.1 Algorithm: Pseudo Code for Time-Lay

```
Technique Base station:
broadcast (Sync_start, level=0)
if receive ( Sync_req) then
send ( Sync_ack , T1, T2, T3)
Neighbour cluster nodes :
receive ( Sync_start , level)
if ( level = null) then
{
```

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

```
level++;
wait a short random time ;
send ( Sync_req, level, T1) ;
receive( Sync_ack);
{
record ( T1, T2, T3, T4);
d = ( (T2 -T1) - (T4 -T3) ) / 2;
calculate (d, )
Sync( d, )
}
Broadcast(Sync_start,node=0)
If node(reciver Sync)
{
Sensor node send(ping)
{
If(Node receive Ping)
{
Send(Ack)
{
Wait for random time
{
Node record(d and d1)
{
IF(d1==d)
{
Node adjust its clock to d
}
Else
{
Reply with Ok message
}
```

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

3.3 Flowchart

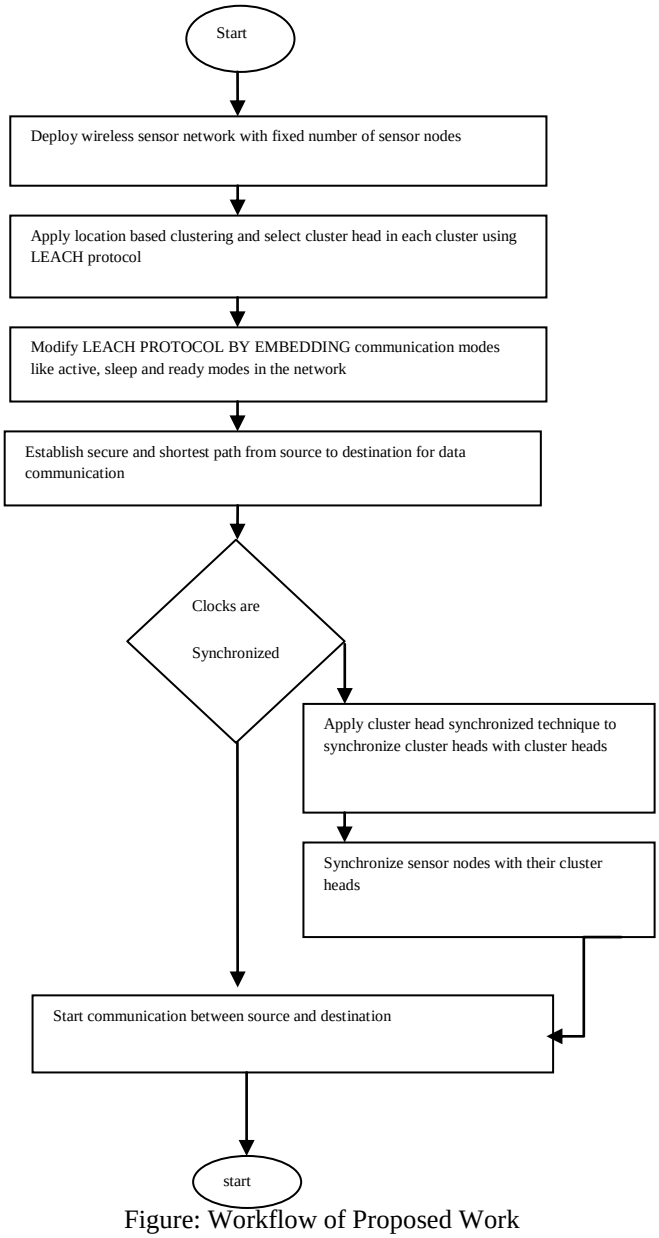

Figure: Workflow of Proposed Work

IV. Experimental Results

The proposed technique is implemented in MATLAB and the results are evaluated in terms of packet loss and throughput. The proposed work has been implemented in MATLAB2015RA. This section presents various results and values of performance metric evaluated. The results obtained are evaluated by using the various performance metrics namely energy, throughput, dead nodes and packet loss (PL). The MATLAB is the tool which is used to perform mathematical complex computations. In this MATLAB simplified C is used as the programming language. The MATLAB has various inbuilt toolboxes and these toolboxes are mathematical toolbox, drag and drop based GUI, Image processing, Neural networks etc. The MATLAB is generally used to implement algorithms, plotting graphs and design user interfaces.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

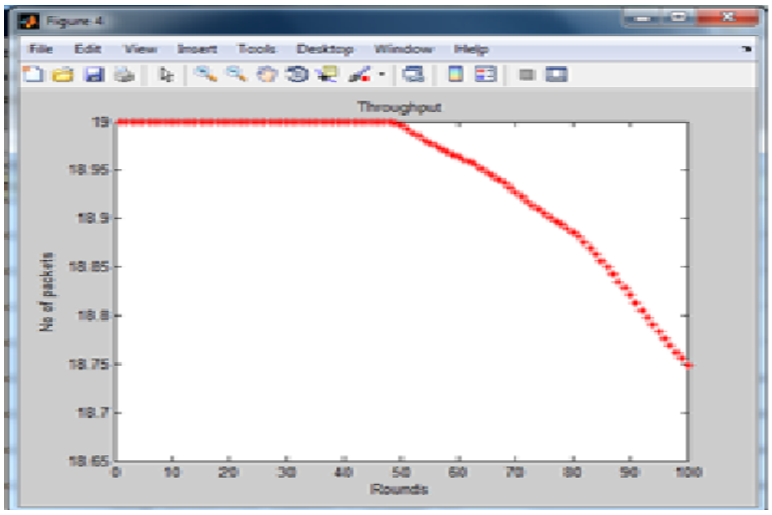

Fig 1: Throughput

As shown in figure 1, the throughput of the proposed technique in which time lay technique is applied for the clock synchronization is analyzed. It is analyzed that throughput is increased at steady rate.

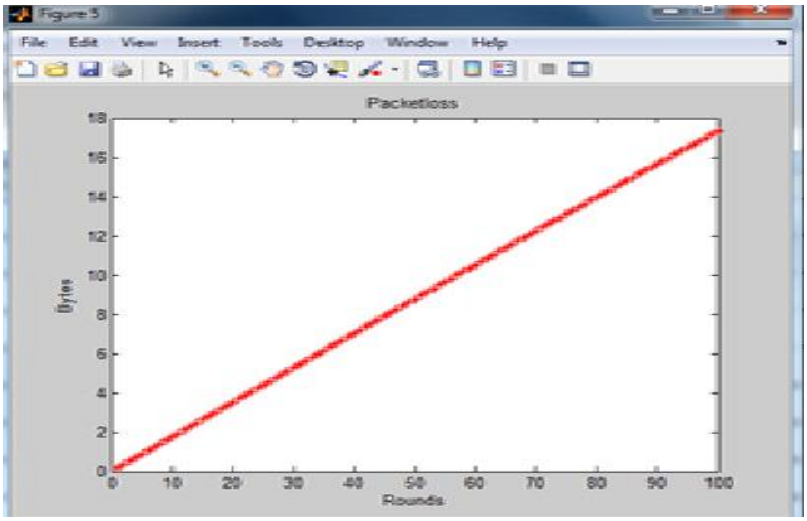

Fig 2: Packet loss Comparison

As shown in figure 2, when the clocks of the sensor nodes are not synchronized then the packet loss may happen. When the clocks of the sensor nodes get synchronized then packet loss in the network get reduced.

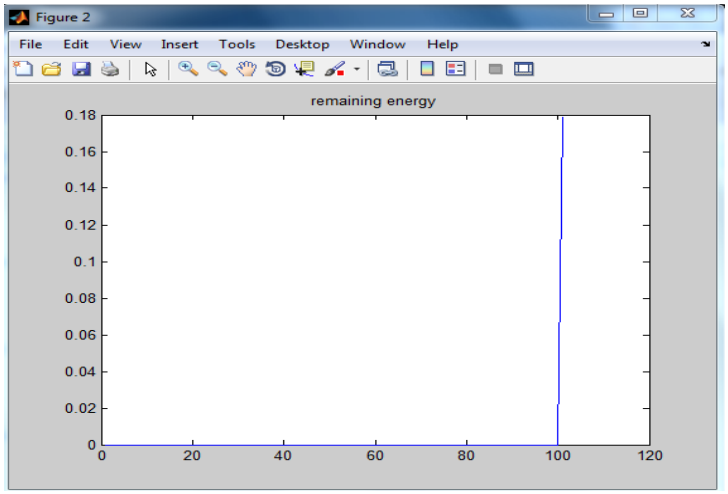

Fig 3: Remaining Energy

DOI 10.17148/IARJSET.2018.5716

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

As shown in figure, the remaining energy with the proposed algorithm is compared with the existing algorithm. It is analyzed that remaining energy with the proposed algorithm is approx 0.18 joules.

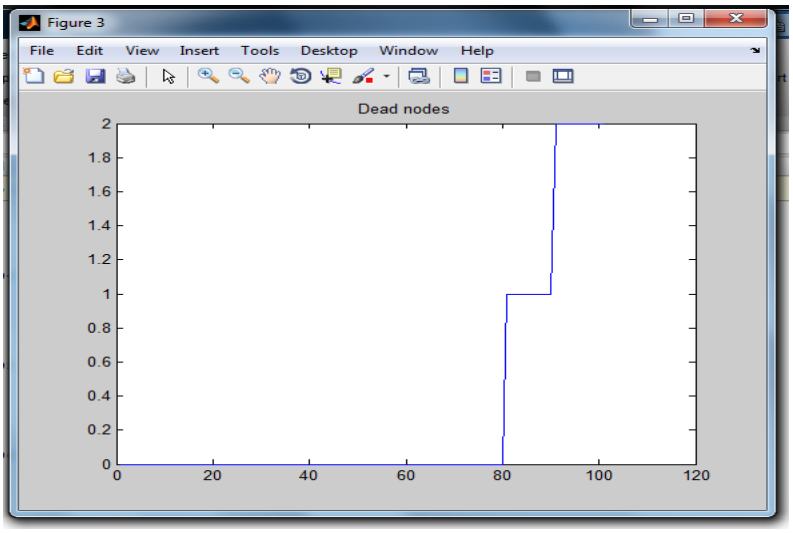

Fig 4: Dead Nodes

As shown in figure, the proposed algorithm performance is analyzed in terms of dead nodes. In the proposed algorithm the number of dead nodes is two.

4.3 Evaluation of Proposed Work

The following section describes the comparison between the proposed work and the existing work. There are four performance metrics which are used for evaluation of work namely energy, throughput, dead nodes and packet loss. The results of the performance metrics show that the proposed work's performance is much better than the existing one in terms of security and efficiency. The results have been tabulated in table 4.1 and the graphical representation of comparison is shown in figure 4.9.

Table 4.1: Table of Comparison

Parameter	Existing Algorithm	Proposed Algorithm
Throughput	17 packets	19 packets
Packet loss	34 Packets	18 Packets
Remaining Energy	0.16 joules	0.18 joules
Number of dead nodes	9 nodes	2 nodes

As shown in table 1, the Proposed and existing algorithms can be compared in terms of throughput and packet loss. The Proposed algorithm performs well in terms of certain parameters. The figure 4.9 shoes the comparison graph.

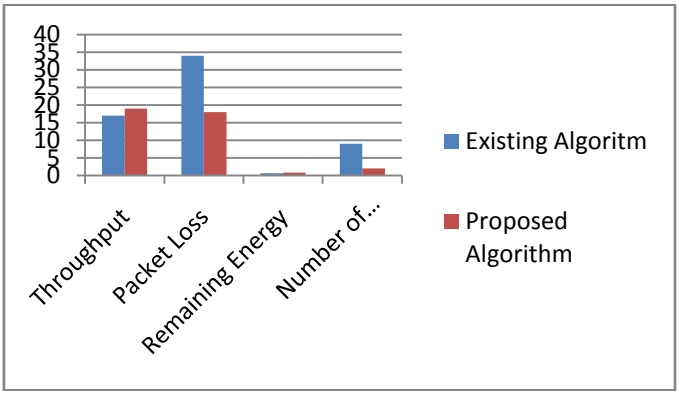

Figure 4.9: Comparison Graph

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

V. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The principle reason for this work is to show which technique is more efficient for clock synchronization of nodes in IOT network. Both the techniques have their own pros and cons. NTP based clock synchronization which make use of GPS increases bandwidth consumption of the network, where as in time lay synchronization technique, all the nodes of the network set their clock according to the third party clock. Hence we can come to the conclusion that both the techniques have their own pros and cons. They can truly profit the IOT world by providing efficient clock synchronization and hence better security. We will come up implementing both the clock synchronization techniques on MATLAB with a specific IOT scenario. For secure channel establishment from source to destination we will implement RSA algorithm. The implemented techniques would then get evaluated on the basis of parameters- number of throughput and packet loss.

5.2 Future Work

Following are the various future possibilities of this research work:-

i. The proposed Algorithm can be further compared with the other algorithm which increases security of IOT.
ii. The proposed algorithm can be further improved to ensure privacy in the network.

REFERENCES

[1] Z. Zhong, J. Peng, K. Huang, and Z. Zhong, "Analysis on Physical-Layer Security for Internet of Things in Ultra Dense Heterogeneous Networks", in Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 39-43, 2016.

[2] T. Charity, H. Hua, "Smart World of Internet of Things (IOT) and It's Security Concerns", in Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 240-245, 2016.

[3] Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things", IEEE Journal of Design and Test, vol. 33, no. 3, pp. 103-115, 2016.

[4] B. Sundaram, M. Ramnath, M. Prasanth, M. Sundaram, "Encryption and Hash based Security in Internet of Things", in Proc. of IEEE International Conference on Signal Processing, Communication and Networking (ICSCN), vol. 3, pp. 1-5, 2015.

[5] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the era of wireless keys: How the IOT can change authentication paradigm," in IEEE World Forum on Internet of Things (WF-IOT). Mar. 2014.

[6] A. Ranjan and G. Somani, "Access control and authentication in the internet of things environment," in Computer Communications and Networks, pp. 283–305, 2016

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[8] P. Wortman, F. Tehranipoor, N. Karimian, and J. Chandy, "Proposing a Modeling Framework for Minimizing Security Vulnerabilities in IOT Systems in the Healthcare Domain", in Proc. of IEEEEMBS International Conference on Biomedical & Health Informatics (BHI), pp. 185-188, 2017.

[9] Z. Guo, N. Karimian, M. Tehranipoor and D. Forte, "Hardware Security Meets Biometrics for the Age of IOT", in Proc. of IEEE International Symposium on Circuits & Systems (ISCAS), pp. 1318-1321, 2016.

[10] T. Abels, R. Khanna, K. Midkiff, "Future Proof IOT: Composable Semantics, Security, QOS and Reliability", in Proc. of IEEE Topical Conference on Wireless Sensor & Sensor Networks (WiSNet), pp. 1-4, 2017.

[11] M. Mohsin and Z. Anwar, "Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IOT Security Analytics", in Proc. of International Conference on Frontiers of Information Technology (FIT), pp.23-28, 2016.

[12] R. Kodali, V. Jain, S. Bose and L. Boppana, "IOT Based Smart Security and Home Automation System", in Proc. of IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1286-1289, 2016.

[13] V. Kharchenko, M. Kolisnyk, I. Piskachova, "Reliability and Security Issues for IOT-Based Smart Business Center: Architecture and Markov Model", in Proc. of IEEE International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), vol. 3, pp. 313-318, 2016.