Secure Channel Establishment Algorithm to Increase Security of IoT

Er. Navpreet kaur[1], Er. Parminder Singh[2]
[1]*Research Scholar,* [2]*Assistant Professor*
[12]*Ramgarhia institute of engineering and technology, Phagwara (RIET)*

Abstract- The IoT is the decentralized network in which the devices can sense information and upload that information to the server. The clocks of the IoT devices are not well synchronized due to which security of the network gets compromised. In this research work, the technique will be proposed which will synchronize clocks of the IoT devices and also establish secure channel from source to destination for data transmission. The proposed improvement leads to increase security of the network and reduce packetloss in the network.

Keywords- IoT, Clock Synchronization, Secure Channel

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 [1]. 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. 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 [2]. 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. 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. There are four security and privacy issues that are found more often. Mostly within the public regions most of the highly distributed IoT devices are deployed such as RFID tags as well as wireless sensors. Thus, the management as well as vulnerability of these devices from physical attacks becomes more difficult. Data integrity has become a concern due to the presence of unattended scenario for IoT devices [4]. A self-supported manner is followed during the operation of most of the devices once they are deployed. In comparison to the supervised wired network, the tampering of data is performed very earlier since there is very little or no maintenance required at all. There is a wireless communication mode utilized amongst the devices as well as gateway. Due to this reason, the confidentiality of data comes to a risk. For instance, within the wireless networks, a major issue that arises is eavesdropping. Due to the presence of resource-constrained types of low-end devices that constitute most of the parts of IoT devices, the confidentiality of the data that is to be transmitted is not easy. In case when the IoT networks are integrated with global internet in order to provide monitoring and interaction with real world, the leakage of information is possible [5]. The data might be accessible to various organizations and domains present on Internet through the connection of real world objects and information. In the 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 [6]. 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. 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

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 [7]. Generally speaking, the method would eventually need to 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.

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 [8]. But the systems have various vulnerabilities as well which might result in causing various issues related to the systems. So, the biometrics provided a proper mechanism for convenience and security within the IoT applications. 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.

T. Abels et.al (2017) IETF impressively defined Internet interoperation crosswise over 30 years of unforeseeable punctuation API. This research reviewed these with streamlining tradeoffs from a bottom up approach utilizing DDS (Data Distribution Service) [9]. At last, additionally work is suggested toward out-of-the-box compos ability and interoperability between normal IoT information models and compliant arrangements. 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.

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 [10]. The attack kill-chain is comprehended along with the leveraging of various attack examples and vulnerabilities. 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 [11]. A smart wireless home security system is highlighted in this paper that sent alerts to the controller when any trespasser was seen within the system. This is done with the help of Internet. The alarm is raised in an optional manner and the concerned systems are notified regarding this issue. 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 [12]. 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. 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.

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.

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:

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

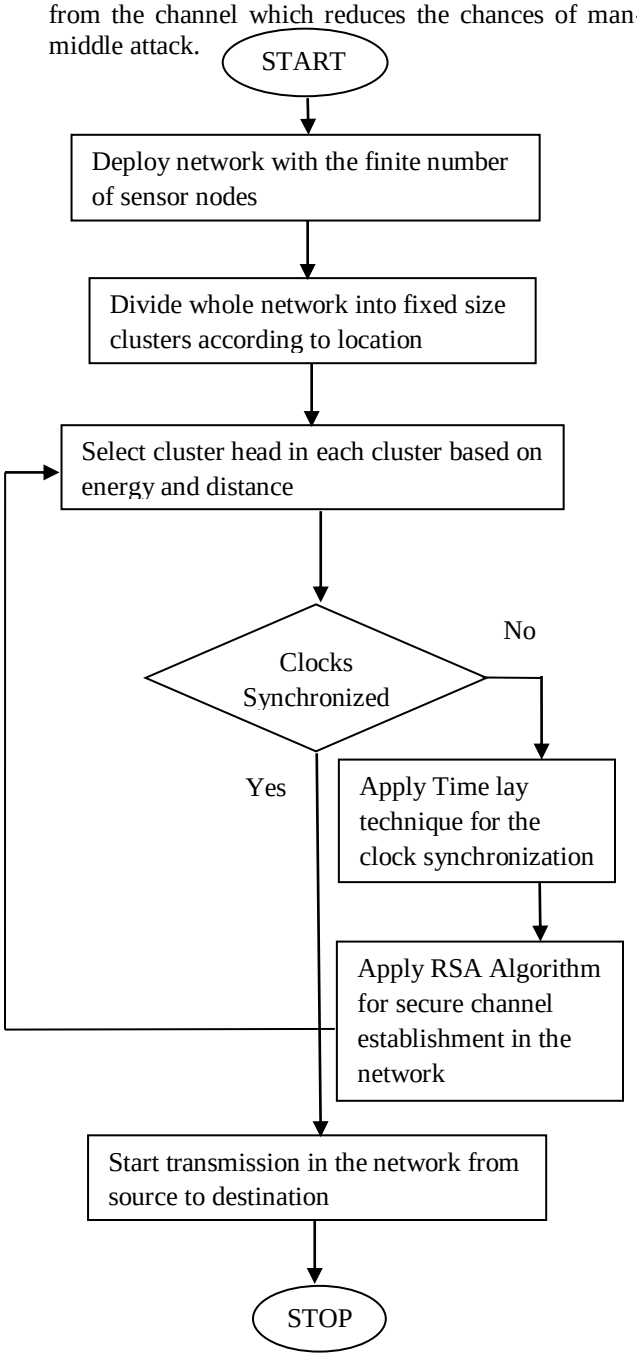

Fig.1: Proposed Flowchart

IV. EXPERIMENTAL RESULTS

The proposed work has been implemented in NS2 and the results have been analyzed by comparing it with exiting technique in terms of energy, throughput and packet loss.

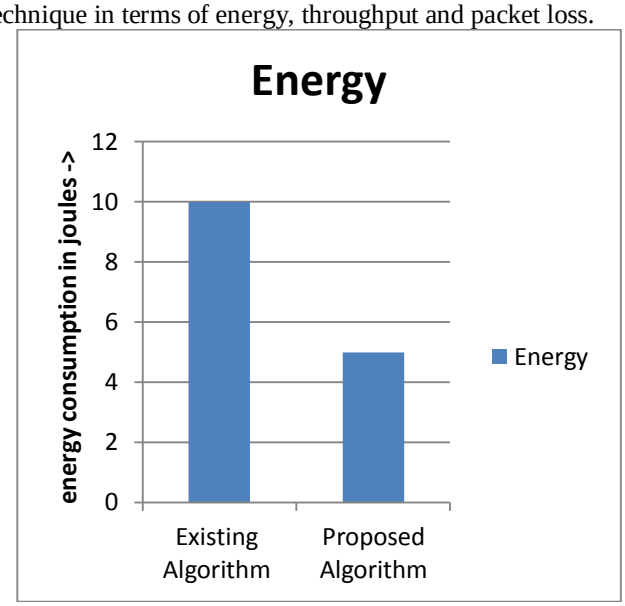

Fig.2: Energy Consumption Comparison

As shown in figure 2, the energy consumption of the proposed and existing algorithms are compared. It is analyzed that energy consumption of proposed algorithm is less as compared to existing algorithm

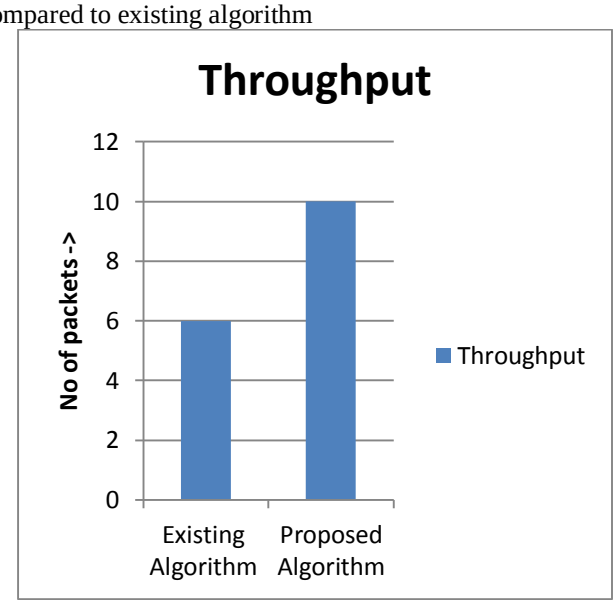

Fig.3: Throughput Comparison

As shown in figure 3, the throughput of the proposed algorithm is compared with existing algorithm. It is analyzed that throughput of the proposed algorithm is more as compared to exiting algorithm

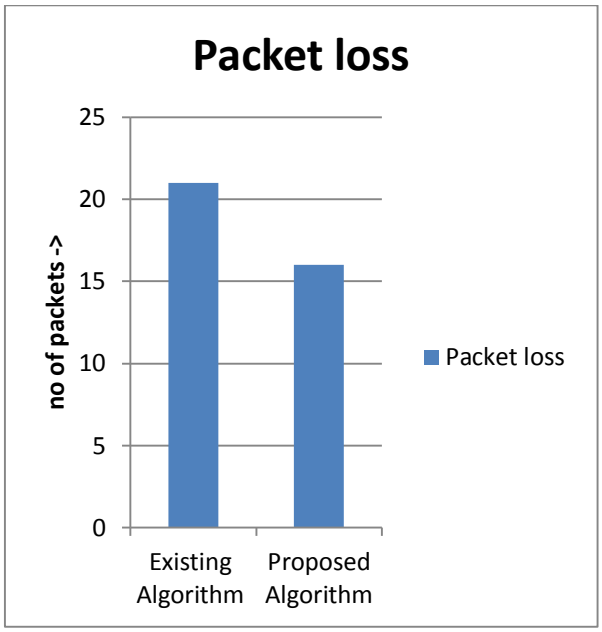

Fig.4: Packet loss Comparison

As shown in figure 4, the packet loss of the proposed and existing algorithm is compared for the performance analysis. The packet loss of the proposed algorithm is less as compared to existing algorithm

V. CONCLUSION

The principle reason for this work is to show which technique is more efficient for clock synchronization of nodes in IoT network. The internet is extended to physical world with the help of IoT technology due to which various security and privacy issues have risen. NTP based clock synchronization which makes 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 NS2 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.

VI. 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), volume 13, issue 45, 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), volume 22, issue 10, 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, no. 18, 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), volume 19, issue 13, pp- 774-785, Mar. 2014.

[6]. A. Ranjan and G. Somani, "Access control and authentication in the internet of things environment," in Computer Communications and Networks, volume 7, issue 9, pp. 283–305, 2016

[7]. 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), vol. 51, iss. 27, pp. 185-188, 2017.

[8]. 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), volume 6, issue 3, pp. 1318-1321, 2016.

[9]. 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), volume 2, issue 19, pp. 1-4, 2017.

[10]. 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), volume 35, issue 85, pp.23-28, 2016.

[11]. 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), volume 45, issue 32, pp. 1286-1289, 2016.

[12]. 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, issue 11, pp. 313-318, 2016.