Time-Lay and RSA Technique for Efficient Data Transmission in Internet of Things

Pankaj Gulati; Amandeep Kaur; Dr. G N Verma
I. K. Gujral Punjab Technical University

Abstract— **Internet of Things (IoT) is a network which is much vulnerable to security attacks due to its decentralized nature. It is a system that connects physical objects which can be accessed through the Internet. These physical objects have large capability to collect and transmit the data over the Internet. For gathering the data from different sources, clocks are needed to be synchronized and security must also be ensured in the network. The modified time lay technique is proposed in this paper which will synchronize the clocks of the IoT devices and maintain a secure channel between the two communicating parties. The simulation modified time technique is performed in NS2 and it is observed that the modified time lay performs well in terms of energy consumption, throughput and delay.**

Keywords— IoT, Secure Channel, Time-lay, Diffie- Hellman, RSA, Encryption, Key management.

I. INTRODUCTION

In the early 1960s a term "Internet" was invented, also known as network of networks. The main purpose of this network was to connect a wide variety of computers through the Internet and provide the data sharing amongst them. The major issue of sharing resources was resolved using the Internet and it also provided the effective results in the research area [1]. The Internet since then has emerged as a widely used technology and is the biggest source of communication through which large number of users can communicate and share their resources. It is coined as a major invention since then and its usage is beyond limits, since near and far communication is possible through this means. It has become a highway where the global world can get connected to each other and provide an effective means to the networking devices and distributing services [2]. In the modern world, size, complexity, and the role an Internet plays have exceeded the initial expectations. Many heterogeneous devices such as wired/ wireless, actuators, sensors and smart home appliances are required to get connected to each other. Various applications are used nowadays to create a smart world where different objects work together to create a context-based application or service. For the physical devices the ever-growing network is the Internet of Things (IoT) [3]. It is a technology that allows users to achieve deep analysis, integration and automation within the system. This technology provides its extension to those devices which require the Internet connectivity for their functions in the system. The embedded technology of Internet has been utilized by many devices in order to communicate with the external environment [4]. It becomes a major concern as well as an opportunity as there is an increase in the data volume and number of connections between various devices. When the IoT services are increased then the large number of devices is designed [5]. In the type of services, security is the major concern of the network. Many levels of configuration and application-level proprietary algorithms are required for the secure communication in IoT-type systems. Due to this security, sometimes user dejects to implement this protection and sometimes provide priority to the functionality over security [6]. This technology is more prone to attacks and thefts due to the unavailability of secured links. Security within these systems is always a major concern as there are numerous systems which are involved in the communication. Thus, the data involved within these systems is to be made secure. As compared to traditional networks, there is much vulnerability in this network like intrinsic characteristics of the IoT, integration of the IoT and the Internet. There are many adversaries that come in the path of IoT network in order to attack an IoT system. Hence, proper evaluation is necessary to overcome such issues in accordance with potential adversarial and information flows in order to avoid those attacks.

The clock synchronization is the real problem because of which it becomes difficult to implement the IoT in a real time system. The efficient communication in the network is done when devices are properly synchronized, which ensures end to end delivery of data without any delay in the network [7]. There are few methods which can be used to get accurate clock synchronization. In Network Time Protocol (NTP)[10], with the use of GPS (Global Positioning System) a proper synchronized time can be attained. The biggest advantage of using NTP system is that it provides high level of accuracy and reliability in terms of clock synchronization. Precision Time Control (PTP)[7] is a protocol which is used to synchronize a clock throughout a computer network. On a local area network, it can achieve time and clock accuracy in a sub-microsecond range which makes it a good match for measurement and control systems [8]. It is basically designed for those applications which cannot afford a GPS tracker at each node. The secure channel establishment is a technique which establishes secure channel from the source to its destination. The Time-lay technique [12] is a technique which is applied for the clock synchronization.

II. LITERATURE REVIEW

T. Inzerilli et al. [9], proposed a location-based approach with the help of which the wireless systems can handle the soft

mobile-controlled vertical handover. There is a detailed analysis of the dual-model terminal that includes UMTS and IEEE 802.11 network interface cards. The good put is optimized and the ping-pong effect is controlled within this novel approach. Depending upon the location of mobile node, the initiation of preliminary handover initiation phase is done. A good put estimation phase that is provided by a transient of casting at the time of soft handovers is followed to perform handover. For attaining handover decisions, the utilization of location information is assessed as per the experimental results.

R. Giuliano et al. [10] focuses on the security aspects of IoT capillary networks. There are both unidirectional as well as bidirectional IP and non-IP devices present within the network. These all are present within the capillary networks and needed a secure access within them. The duration of the validity of the time window is assessed within this paper. Results are examined in terms of the time required for transmission within the realistic scenario along with the indication for setting time limit for the validity of the window. At the end, the benchmark analysis is provided for assessing the effectiveness of the proposed method in terms of security when various attacks were present in the scenario.

R. Giuliano et al. [11] presented as analysis which highlight various security guidelines of the IoT capillary network. The algorithm is proposed in this paper which provides security to uni-directional and bi-directional devices. The secure channel which is established to provide security will be renewed after certain amount of time. The effectiveness of proposed technique is assessed along with the analysis of security by providing the analysis of benchmark through the comparisons against existing techniques.

Iqbaljeet et al. [12] stated that Wireless Sensor Network has no central controller, due to which energy consumption is a major issue. By using Bully algorithm, greater probability of becoming Cluster Head is given to node with higher energy for better distribution of energy and more reliable message transmission. In this paper, author had used the diffusion based technique to synchronize cluster head clock. As per the simulation results, it is analyzed that proposed algorithm increase efficiency of the network in terms of energy, packet loss and delay.

A. Tekeoglu et al. [13], proposed a testbed for examining the security and privacy of IoT devices. Here, layer 2 and layer 3 packets are captured within this testbed. The security and privacy related issues within various IoT devices are investigated. Various vulnerability related scans, identification of insecure protocol versions, firmware updates, and various other issues related to authentication and privacy are performed within the testbed. It is seen that the proposed system provides better performance in terms of security parameters like authenticity and privacy

I. Nasr et al. [14] proposed a clock synchronization algorithm which is based on the non coherent timing detection. The coherent timing detectors work on the Rayleigh fading channel technique for the clock synchronization in the IoT. The Rayleigh fading channel technique is very light weight due to which the complexity of the system reduced to greater extent. The proposed technique performs well than the NDA (Non Data Aided) coherent technique for clock synchronization in term of mean square error.

The performance of the proposed technique was analyzed in terms of MSE (Mean Square Error) and it had been analyzed that it performs better than NDA (Non Data Aided) Coherent technique for clock synchronization.

III. PROBLEM STATEMENT

The clock synchronization is the issue of IoT networks. To resolve the issue of clock synchronization, NTP protocol came into existence which uses GPS system to synchronize clock of the IoT devices. Following are the various drawbacks of NTP protocol:

1. The NTP protocol uses the GPS system for the clock synchronization. In the IoT, the mobile devices are used for communication due to use of GPS system, the energy consumption is increased which reduces the network lifetime.
2. The NTP protocol is based on synchronizing clocks of IoT devices and use external control messages which increase routing overhead and delay in the network.
3. Time-lay technique is one of the clock synchronization technique used in WSN. In this all the nodes of the network set their clock according to the third party clock. and it has following advantages over NTP:
4. The Time-lay technique does not use the external message or device for clock synchronization which reduces delay and routing overhead for clock synchronization as compared to NTP protocol.
5. The IoT is the decentralized network due to which mobile devices keep on joining the network and in this technique cluster head takes initiative for the clock synchronization which is energy efficient approach as compared to NTP protocol.
6. It is analyzed that the Diffie- Hellman has high complexity for the secure path establishment as compare to RSA algorithm.

IV. PROPOSED METHODOLOGY

This work is based on clock synchronization and secure channel establishment for communication in IoT. For this, firstly we deploy the sensor network with finite sensor nodes. In WSN, time-lay technique is used to synchronize the clocks by taking base station as the initiator. To introduce the clock synchronization, the technique of Time-lay will be used in

which all the nodes of the network set their clock according to the third party clock. Here all the sensor nodes are grouped into clusters and each cluster has one base station. Each node of the cluster sends clock time to the base station. After that base station will calculate the average clock time and set their clock according to average clock. Similarly the other clusters of that network calculate their average clock time. Now to synchronize with the network, all the base stations will share 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. It works in two phases: The *level discovery phase*, followed by the *synchronization phase*. The pseudo code is explained as follow:

Level discovery phase: The level discovery phase is based on constrained flooding. The root node is assigned level 0; this node initiates this phase by broadcasting a level-discovery packet that contains the identity and the level of the sender. The immediate neighbours that receive this packet assign themselves a level that is one greater than the level in the packet received (i.e., level 1 in this case). After this step, these neighbours broadcast a new level-discovery packet with their own level. This process is continued until each node has a level.

Synchronization phase: Consider a message exchange between two nodes A and B, as shown in Fig. 3.1. T1 and T4 represent the time measured by A's local clock. Similarly, T2 and T3 represent the time measured by B's local clock. We assume that A's level is greater than B's by one.

1. At time T1, A sends a synchronization-pulse message to B. The synchronization-pulse message contains the level number of A and the value of T1. Node B receives this packet at T2, where T2 = T1 + d and d represents the clock offset between the two nodes.
2. At time T3, B sends an acknowledgement packet to A. This packet contains the level number of B and the values of T1, T2, and T3. With this information, node A calculates the clock offset as follows:
   d= ((T2-T1) - (T4-T3)) / 2
3. Node A corrects its clock to synchronize with node B, based on the computed offset.

A. RSA Algorithm

An asymmetric encryption algorithm which was proposed in 1978 and was mostly accepted and implemented within the public applications, is known as the RSA algorithm. This type of algorithm can be utilized for both data encryption as well as digital signature.

a. Advantages:

- The RSA algorithm uses the asymmetric cryptosystem which is more secured as compared to symmetric cryptosystems.
- The algorithm is secure as it reduces the chances of the man-in-middle attack.

Pseudo code for Modified Time-lay technique

```
Cluster Head:
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
{
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, )
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
}
```

V. RESULTS & DISCUSSION

The Internet of things is different from the wireless sensor networks. Due to difference between architecture of WSN and IoT, routing protocols are different. In the wireless sensor networks LEACH is used as the routing protocol and in IoT RPL [5] is used as the routing protocol. In this research work, the directed communication takes place in the network which is not possible in WSN. The performance of proposed modified time-lay algorithm is compared with the existing

scenario as mentioned in [11], in which NTP (Network Time Protocol) is used for clock synchronization and Diffie-Hellman for secure channel between IoT devices. The performance of proposed algorithm is compared with the scenario where no clock synchronization ad security algorithm is implemented. The modified time-lay technique is implemented in NS2 with parameters stated in Table 1, and results are analyzed in terms of delay, throughput and energy consumption.

Table 1: Simulation Parameters

Parameter	Value
No. of nodes	80
Topography Area	1500m ×1200m
Channel type	Wireless
Antenna Type	Omni-directional
Queue Type	Priority Queue
Queue Size	100 packets
Link Type	LL
MAC Layer	IEEE 802.11g
Routing Protocol	RPL
Transmission Range	140 m
Traffic Type	Constant Bit Rate (CBR)
Simulation Time	100 seconds
Simulation Tool	NS 2.35

Following are the parameters used for evaluating the proposed work:

A. Energy Consumption: The energy is performance analysis parameter which measure energy consumption of the network. The energy consumption of the network is measure with the number of packets multiplied with per unit energy. The network is efficient when it has least energy consumption

Energy consumption= number of packets transmitted x per unit energy

B. Throughput: The amount of data being transmitted in a given period of time from one region to the other is calculated by throughput.

Throughput= (number of packets received / number of packets sent)×100

C. Delay: The delay is the parameter which count delay in the data transmission. The delay can be calculated with the time at which packet received minus time at which packet sent.

Delay = Time at which packet received- Time at which packet sent

It is observed from figure 1, that the time-lay offers a superior throughput rate than NTP and other case in which no technique is applied. It is noticed that the throughput mainly increases after 40 seconds because till that the base station floods the control messages in the network for topology discovery.

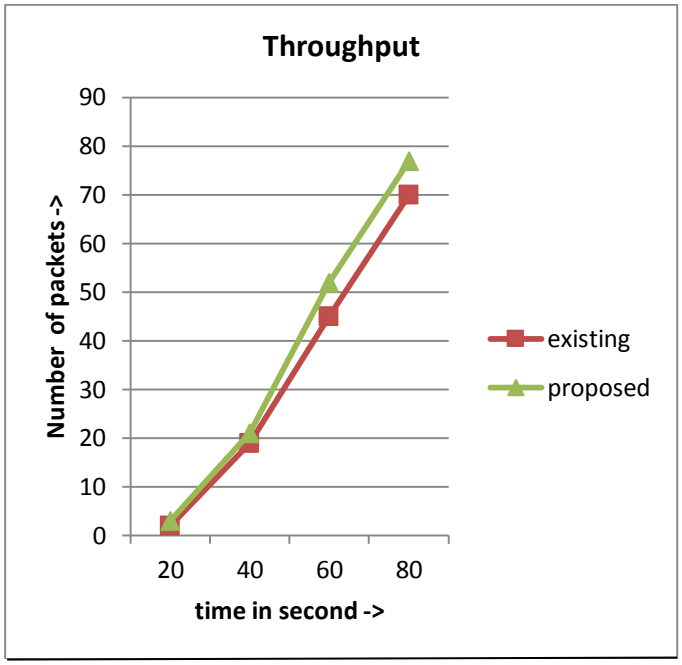

Figure 1: Throughput Comparison

As shown in figure 2, GPS system uses Internet to synchronize the clocks, due to which energy consumption is more in NTP. Whereas in time-lay number of messages exchanged are more but even then the energy consumption is less as shown in figure 3 due to which there is slight variation. The energy consumption is less because less number of messages are exchanged in the NTP technique.

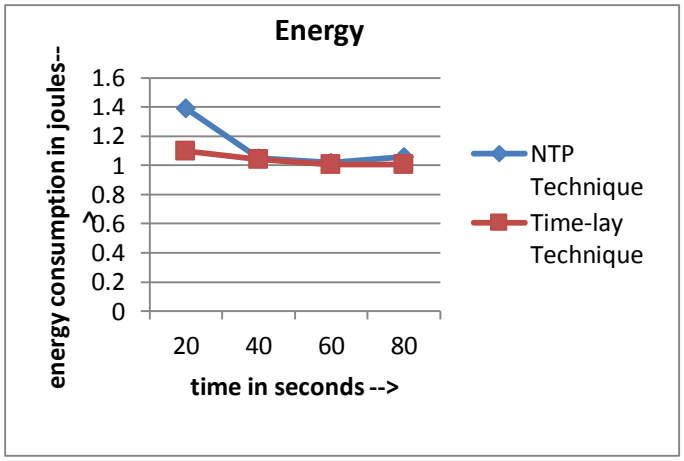

Figure 2: Energy Comparison between NTP and Time-lay

It is observed from figure 3, that the time-lay offers least delay than NTP and other case in which no technique is applied. It is noticed that the delay mainly decreases after 40 seconds because till that time, the base station floods the control messages in the network for topology discovery.

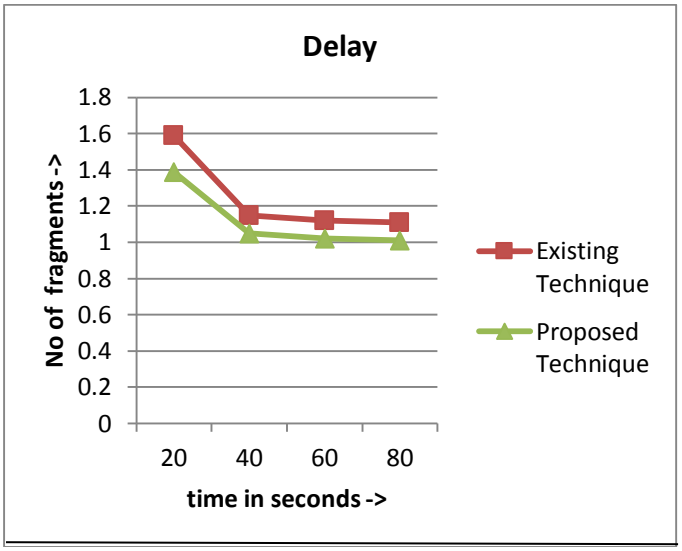

Figure 3: Delay Comparison

The measures of our performance metrics that are energy, throughput and delay are stated in Table II.

Table II: Table of Comparison

Time	Without any technique	NTP Technique	Time-lay Technique
Energy Consumption			
20	90	1.39	1.10
40	60	1.05	1.04
60	80	1.02	1.006
80	100	1.06	1.004
Throughput			
20	2	2	3
40	13	19	21
60	33	45	52
80	48	70	77
Delay			
20	2.39	1.59	1.39
40	2.05	1.15	1.05
60	2.02	1.12	1.02
80	2.01	1.11	1.01

VI. CONCLUSION

In this paper, it has been concluded that Internet of Things is a type of network in which information which is accessed from the sensors are passed to the base station. To efficiently collect the data from the sensors, clocks of nodes are needed to be synchronized. In this research, a modified time-lay technique is applied which is used to synchronize the clocks of the devices. The RSA algorithm is used which can encrypt and decrypt the information which is transmitted over the channel. It is seen through the simulations that the modified time lay technique performs well in terms of energy, delay and throughput

REFERENCES

[1] R. Giuliano, F. Mazzenga, A. Neri, A. Vegni, and D. Valletta, *"Security implementation in heterogeneous networks with long delay channel"*, in Proc. of IEEE AESS European Conference on Satellite Telecommunications(ESTEL), vol. 1,pp. 1-6, 2012.

[2] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, *"Security, privacy and trust in Internet of Things: The road ahead,"* Journal of Computer Networks, vol.76, pp. 146-164, 2015.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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

[8] 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.

[9] T. Inzerilli, A. M. Vegni, A. Neri, and R. Cusani, "A Location-based Vertical Handover algorithm for limitation of the ping-pong effect", *in Proc. of IEEE*

International Conference on Wireless & Mobile Computing, Networking & Communication, vol. 14, no. 7, pp. 108-117, 2008.

[10] R. Giuliano, F. Mazzenga, A. Neri, A. M. Vegni, "Security Access Protocols in IoT Networks with Heterogenous Non-IP Terminals", *in Proc. IEEE International Conference on Distributed Computing in Sensor Systems*, vol. 5, no. 12, pp. 323-336, 2014.

[11] R. Giuliano, F. Mazzenga, A. Neri, A. M. Vegni, "Security Access Protocols in IoT Capillary Networks", *IEEE Internet of Things Journal*, vol. 19, no. 4, pp. 160-168, 2016.

[12] Iqbaljeet, S. Rana, "A Novel Technique for Clock Synchronization to Increase Network Lifetime in WSN", *International Journal of Computer Science and Engineering*, vol. 4, no. 3, pp. 106-110, 2016.

[13] A. Tekeoglu, A. Tosun, *"A Testbed for Security and Privacy Analysis of IoT Devices",* in Proc. of IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), vol. 13, pp. 343-348, 2016.

[14] I. Nasr , L. Atallah , S. Cherif and B. Geller, *"Time synchronization in IoT Networks: Case of a Wireless Body Area Network",* IEEE Internet of Things Journal, vol. 14, no. 5, pp. 864-949, 2016.