Angle of Trajectory Technique for Efficient Handoff in IOT

Amarendra Kumar[1], Ankit Kumar[2]
[1]*Research Scholar,* [2]*Assistant Professor*
[12]*CBS Group of Institution, Jhajjar, Haryana*

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- Hand Off, Angle of Trajectory, Soft handoff

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 development of Internet has been since the 1970s and has grown around 1980s. However, its usage has mainly grown worldwide within the 1990s [1]. 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. 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. 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 [3]. A 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 [4]. Further, the features such as low latency, higher efficiency, less cost and many more are applied with the help of by-hop. However, each node might get plaintext message through utilization of

by-hop encryption due to the decryption operation within transmission node. Thus, there is need of high credibility of transmission nodes within by-hop encryption. On the basis of type of business, separate security policy can be selected through the utilization of end-to-end encryption. Thus, for the high security requirements of business, high level security protection can be provided by this approach. The encryption of destination address cannot be provided by end-to-end encryption since on the basis of destination address, the transmission of messages can be known for each node. The malicious attacks can thus be caused since the message being transmitted at source and destination cannot be hidden [5]. It can be concluded here that the by-hop encryption protection can be applied when there is less level of security requirement of any business. The end-to-end encryption can be applied further when higher security level is required for business. 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. 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 [6]. 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. Coupled with the growth of information passed through these embedded systems, there was a clear and potential danger in having these IoT devices and networks not be held to indistinguishable rigorous standards of design from other industrial-level technology. 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]. 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. There is a need of proper communication amongst the devices and humans in case of IoT systems for their proper usage. So, the biometrics provided a proper mechanism for convenience and security within the IoT applications [8]. 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. 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 [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 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.. Further the network semantics are aligned for providing appropriateness within the IoT systems [10]. 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. For the purpose of making an application smarter, safer and automated there was a need to enhance the working of such applications. 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 [11]. 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 SBC is designed in such a manner that the hardware and software mechanisms are seen by the manufacturers in a proper manner [12]. 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

The sensor nodes which sense the information is passed to the base station. The sensor nodes are mobile in nature, due to which handoff is required in the network. There are two types of handoff's. The first handoff is hard handoff in which packet dropping is possible and on the other hand, the soft handoff do not have any packet drop and delay. In the existing technique, the IPv6 technique is applied which leads to hard handoff and in this research angle of trajectory technique will be applied which leads to soft handoff. Trajectory is the path followed by a projectile an object in motion. A projectile is further defined as an object propelled with some initial velocity and allowed to be acted upon by other forces including gravity and air resistance.

A trajectory has horizontal (x) and vertical (y) position components.

The units of both horizontal and vertical positions are considering in meters (m).

If we know either vertical or horizontal position than by the use of that we can find the other position. Like if we know the values of horizontal position than we can calculate the value of vertical position.

Formula:

$$vertical\ posotion(y) = \big((x)(\tan\theta)\big) - \left(\frac{(a)(x)}{2(v)^2(\cos\theta)^2}\right) \quad (5)$$

Where x denotes horizontal position,

$\tan\theta$ denotes tangent of launch angle

V denotes initial velocity and $\cos\theta$ denotes cosine of launch angle.

The following figure describes proposed work step by step:

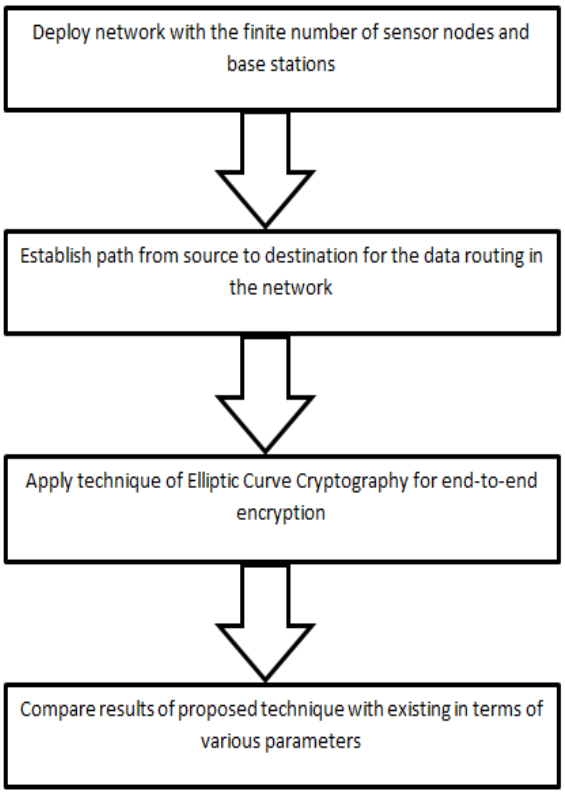

Fig.1: Flow Chart of Proposed Work

Experimental Results

The proposed algorithm is implemented in NS2 and the results are compared with existing algorithm to analyze the performance in terms of throughput and energy consumption.

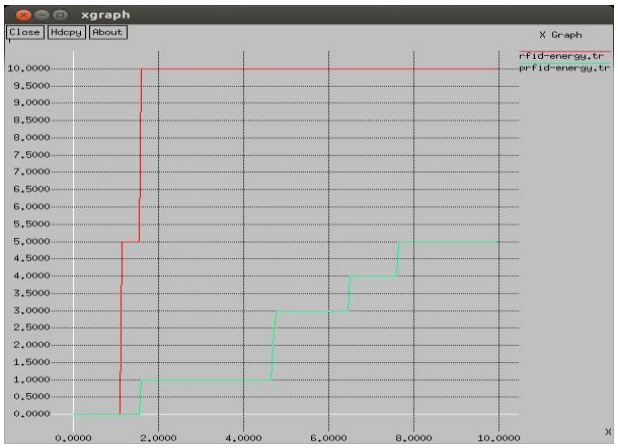

Fig.8: Energy Consumption

As shown in figure 8, the energy consumption of proposed algorithm is compared with the existing algorithm. It is analyzed energy consumption of proposed algorithm is less as compared to existing algorithm.

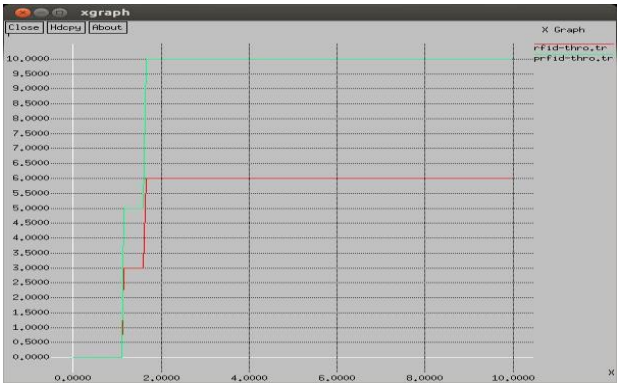

Fig.9: Throughput Comparison

As shown in figure 9, the network throughput is compared with the existing technique. It is analyzed that network throughput is more as compared to existing technique.

IV. CONCLUSION

In this paper, It is concluded that IoT is the network which is decentralized in nature and sensor nodes can change its location any time. The sensor node sense information and pass information to base station. The sensor nodes has mobile in nature which can change it location any time. In this research work, technique of angle of trajectory technique is proposed for efficient hand off in the network. The proposed algorithm is implemented in NS2 and simulation results shows high performance as compared to existing technique.

V. REFERENCES

[1]. O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen,"Capillary Networks – Bridging the Cellular and IoT Worlds", in Proc. of IEEE World Forum on Internet of Things, vol. 2, pp. 571-578, 2015.

[2]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements and future direction", Journal of Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, 2013.

[3]. H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, pp. 648-651, 2012.

[4]. J. Granjal, E. Monteiro, and J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in Proc. of IEEE on Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.

[5]. 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.

[6]. 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.

[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), 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), 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), 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), 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), 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, pp. 313-318, 2016.