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

A Review of Enhancement in Security frame Work for Bi-directional Communication with Clock synchronization in Internet of Things

Satwinder Kaur[1], Ms. Amandeep Kaur[2]

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

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

ABSTRACT

The Internet of things (IoT) is the network in which sense information is passed to the base station (BS) and base station (BS) 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 will be proposed which is based on secure channel establishment and symmetric key cryptography.

Index terms: - Internet of thing (IoT), Base station (BS).

I. INTRODUCTION

The internet is a global system of interconnected computer network that utilize the standard internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of millions of private, public, academic, business, and government networks, from local to global in scope. Originating from the Advanced Research Projects Agency Network (ARPANET) around 1970, it was available in the 1980s and got to be famous around 1990. The Internet of Things (IoT), otherwisecalled the Internet of Objects, alludes to the networked interconnection of regular objects. Today, the Internet of Things has turned into a leading path to the smart universe of ubiquitous computing and networking. A network of interconnected computers speaks with a network of interconnected objects continually tracking and accounting for millions of things, from razor blades to banknotes to auto tires [1]. There are many applications where it is widely used like smart home, forestry monitoring, intelligent transportation, wisdom medical, industrial automation et cetera [2]. As mentioned in the introductory section of the paper Archudha Arjunasamy. et, al [3]. Intelligent transportation: Mainly to monitor the traffic conditions and providing data for traffic management or reference recommendations for drivers. The system designed in research consists with fixed roadside detection units, on-board units located in the vehicles, backend server and the client terminals. The system obtains the road picture information through the cameras on roadside keeping in mind the end goal to decide the weather and road conditions, and obtains the temperature, speed and position information of every vehicle through on-board units. Minchul Shin. et,al (2016)

[4] In this paper survey the Granularity of the resources ought to be based on the complexity of the structure and

function. The fine grain resources more often than not have basic structure and single function, which can be further divided into sensors, controllers and RFID equipment as indicated by the resource type.Kun Wang.et, al (2016) [5].In this paper id based on the Access Capabilities At present, things in IoT are chiefly composed of equipment and resources which can access the IoT and can process a wide range of information. For instance, a smart telephone or a computer can depend all alone hardware and software resources to access the IoT, and some industrial equipment that supports M2M technology can likewise access the IoT with the assistance of communication resources.Dongsik Jo. et,al (2016) [6] The identification ought to be unique, traceable and controllable. This process involves the registration mechanism, authentication mechanism, and information transmission security and other related technologies. Jun Qi, Po Yang,et, al (2016) [7]. In the non-functional requirements, the access restricted devices mostly expand their software and hardware resources for the performance requirements. Some access restricted devices are restricted by their hardware resources. For instance, some sensor networks are limited in calculation and storage performance, and some industrial controllers are absence of communication capability.

II. LITREATURE SURVEY

H. Suo, J. et.al, "Security in the Internet of Things: A Review," 2012

In the previous decade, internet of things (IoT) has been a concentration of research. Security and privacy are the key issues for IoT applications, and still face some enormous challenges [8]. By method for deeply breaking down the security architecture and feature, the security requirements are given. On the premise of these, the research issues of key technologies is talked about including encryption mechanism, communication security, protecting sensor data and cryptography algorithm, and quickly outlines the challenges.

J. Granjal, et.al, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," 2015,

This survey breaks down existing protocol and mechanism to secure communications in the IoT, and in addition open research issues.The Internet of Things (IoT) introduces a vision of a future Internet where clients, computing frameworks, and regular objects having sensing and actuating capabilities cooperate with unprecedented convenience and economic benefits [9].

L. Atzori, et.al, "The Internet of Things: A survey", Computer Networks", 2010

The most important aspects of the IoT are surveyed with emphasis on what is being done and what are the issues that require additionally research. This paper addresses the internet of things. Fundamental enabling factor of this promising paradigm is the integration of several technologies and communication solutions. Identification and following technologies, wired and remote sensor and actuator network, enhanced communication protocol, and distributed intelligence for smart object are only the most relevant [10].

O. Novo, et.al, "Capillary Networks – Bridging the Cellular and IoT Worlds," 2015

As a result, a vast range of constrained devices equipped with just short-range radio can use the cellular network capabilities to increase global connectivity, supported with the security, management and virtualization services of the cellular network [11].

R. Giuliano, et.al, "Security implementation in heterogeneous networks with long delay channel," 2012

In this paper, the security issue is tackled for non-IP devices ready to connect by a short-range with a mediator gateway, forming a capillary access network, which can be viewed as a short range extension of traditional access network keeping in mind the end goal to efficiently capture the IoT movement. In particular, security algorithms are proposed both for uni-directional and bi-directional terminals, contingent upon the terminal capabilities [12].

S.Sicari, et.al, "Security, privacy and trust in Internet of

Things: The road ahead," 2015

In this situation, the fulfillment of security and privacy requirements plays a fundamental role.Such requirement incorporate data confidentiality and authentication, access control inside the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. More in subtle elements, a unified vision regarding the insurance of security and privacy requirements in such a heterogeneous environment, including different technologies and communication standards is as yet lost [13].

R. H. Weber.et.al, "Internet of Things – New security and privacy challenges," 2010

The internet of things is an emerging global. From a technical point of view, the architecture depends on the data communication tools, primarily RFID tagged items. The IoT3 has the purpose of providing an IT-foundation

encouraging the exchanges of "things" in a secure are reliable manner. Measures ensuring the architecture's resilience to attack, data authentication, access control and client privacy should be established [14].

J. Yun, et.al, "A Device Software Platform for Consumer

Electronics Based on the Internet of Things", 2015

This paper proposes a one M2M standards-compliant device software platform for consumer electronics in light of the Internet of Things, called &Cube. It leverages a standardized resource model and REST APIs to work with one M2M service platforms, prompting to interoperability crosswise over various IoT consumer electronics built on the &Cube [15].

III. PROTOCOL FOR SECURITY NETWORK ACCESS

They are three types of security network access.

A. Time based secure key Generation and Renewal

Time based secure key to provide the secure connection and there is no need of a server that manage the secure key. The main characteristics, the local key synchronization and generation occur by means of the generation of symmetric encryption key at both sides of communication channel. Are not shared along the connectivity link.

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

B. Security Access Algorithms for Bi-directional Data Transmissions

Bi-directional data transmission each device can send and receive packets. The mediator can periodically broadcast its clock timing in a dedicated message, and its identity in a plan part of message. In this case gateway/ mediator, propagation delay can be neglected.

C. Security Access Algorithms for Uni-directional Data Transmissions

Uni-directional devices cannot perform any secure procedure for secure key exchange with the mediator. The transmitter send a message without any feedback and it fails to receive any signal is equipped with an internal clock, assumed as not accurate.

IV. BOOTSTRAP PROCEDURE

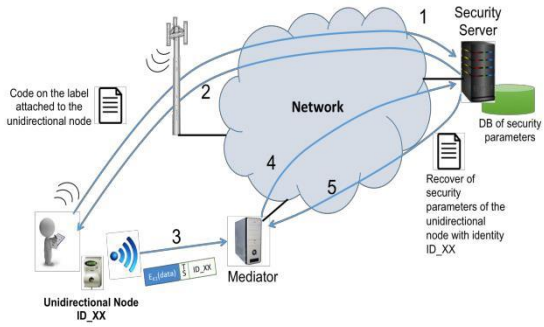

Figure: Bootstrap procedure for unidirectional devices

This procedure can be different for uni-directional and bi-directional nodes due to different communication capabilities.

Bootstrap procedure for uni-directional nodes is depicted in figure. The human installer, who read the code on the label attached to the node, and communicates it to the security server by using the mediator or any other access technology, such as the available cellular radio link (step 1). The installer is the acknowledged by the security server (step 2) The security server generates all above security parameters related to the new installed nodes, and store them in the local database.

When mediator receives for the first time an encrypted message by the new nodes (step 3), it retrieves all associated security parameter by interrogating the security server (step 4 and step 5). At the end bootstrap procedure, the mediator is able to correctly decrypt the message by the new node.

The proposed algorithm is being implemented under the simulated environment. It is being analyzed that proposed algorithm performs well in terms of energy consumption, throughput and delay

V. CONCLUSION

The internet of things is the techniques in which the sensed information is passed to the internet to perform required tasks. In the internet of things has decentralized architecture due to which security, routing and quality of services are the three major issues of this network. In this paper, various techniques which in the recent times to resolve security issues has been reviewed and discussed in terms of various parameter.

VI. REFERENCES

[1] D.P.F. Moller, *"Introduction to the Internet of Things"*, 2016, Springer International Publishing Switzerland, 978-3-319-25178-3_4

[2] Shulong Wang, Yibin Hou, Fang Gao1 and Xinrong Ji, *"Access Features Analysis of Things in the Internet of Things"*, 2016, IEEE, 978-1-5090-2534-3

[3] Archudha Arjunasamy, Thangarajan Ramasamy, "A Proficient Heuristic for Selecting Friends in Social Internet of Things", 2016, ISCO, 3294794

[4] [Minchul Shin, Inwhee Joe, "Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things", 2016, IET Commune., Vol. 10, Iss. 12, pp. 1508–1521

[5] Kun Wang, Xin Qi, Lei Shu, Der-Jiunn Deng, and Joel J. P. C. Rodrigues, *"Toward Trustworthy Crowdsourcing in the Social Internet of Things",* 2016, IEEE, 1536-1284

[6] Dongsik Jo and Gerard Jounghyun Kim, *"ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere"*, 2016, IEEE Transactions on Consumer Electronics, Vol. 62, No. 3

[7] Jun Qi, Po Yang, Martin Hanneghan, Dina Fan, Zhikun Deng, Feng Dong*, " Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment"*, 2016, IET Net., Vol. 5, Iss. 5, pp. 107–113

[8] 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

[9] 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

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

[11] 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

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

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

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

[15] 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