Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 12, December 2018, pg.150 – 153

Energy Efficient Techniques of IoT: A Review

Neha Sharma
Research Scholar, Bahra University, Waknaghat, Shimla Hills
nehasharma7576@gmail.com

Parul Gazta
Assistant Professor, Bahra University, Waknaghat, Shimla Hills
parulgazta@gmail.com

Abstract: The IOT network is the decentralized type of network which can sense the information and pass it to base station. Due to small size of the sensor nodes, the energy consumption is the major issue of the network. The LEACH is the energy efficient protocol which can divide whole network into fixed size clusters. In each cluster, cluster heads are selected which can transmit data to base station. The various clustering techniques are proposed so far to improve lifetime of IoT. In this review paper, energy efficient techniques of IoT are reviewed and analyzed in terms of certain parameters

Keywords: LEACH, IoT, Energy efficient

Introduction

IoT stands for internet of things which is termed by the of the Radio Frequency Identification (RFID) development community in 1999. The application of the IoT is widely used in many applications due to large growth of mobile devices, embedded and omnipresent communication, cloud computing and data analytics [1]. Large numbers of devices are connected over public or private Internet Protocol networks with the help of billions of objects can sense, communicate and share information. The data collected by these interconnected devices continuously, after which it is analyzed to perform action in order to provide a wealth of intelligence for planning, management and decision making. The main objective here is to interconnect all the things present within this self-configuring wireless network which includes numerous sensors. An object that gets involved within a communication chain is also present. The combination of communication capabilities which are given by the data transmission is given by these lines present. RFID is known to be the main object within the IoT. The building of global infrastructure for RFID tags which is known to be a wireless layer present on the top of Internet [2]. The communication is made amongst network of interconnected objects and the interconnected computers. There is a different Internet Protocol (IP) location for the objects at some instants. These objects are embedded within the complex systems. In order to gather the information here, the various sensors are used which gather information related to temperature, and other aspects present in the surroundings. The sensors present near to each other transfer the gathered information in order to

provide further processing as per the requirements of the current applications. Cloud computing is a highly scalable and cost-effective infrastructure for running number of applications such as HPC, enterprise and Web applications. However, there is one big critical issue in cloud computing which have been emerging due to its growing demand which have drastically increased the consumption of energy in data centers [3]. The issue of high consumption not only increase the operation cost which reduces the profit of cloud providers but it also affect the environment as the high consumption of energy leads to high emission of carbon. Hence, energy-efficient solutions are required to minimize the impact of Cloud computing on the environment. At the different layers of IoT framework security is the major requirement. The need of the security in IoT framework can be illustrated by identifying the layer wise security requirements. Perception layers, security requirements are data privacy by which only authorized user can read or write data and user is guaranteed about the privacy of their data that no one can utilized their data without proper access permission [4]. For the authentication cryptography hash algorithm has been utilized that provides risk assessment and authentication to the user. With the help of this, device can authenticate and verify that with whom it is interacting is authentic person. Middleware layer is the layer in which it is necessary to access the error free information or data by the authorized person immediately [5]. It is necessary to check the availability of devices I order to know vulnerabilities. Data redundancy monitored every transmission in network and helps in preventing the denial attacks. Application layer, security requirements of the application layer are authentication, risk assessment, data security for the protection of digital content which is very necessary in order to secure environment. It involves the authentications of externals that can permit permission to the data and information. Misdirection attack is the attack in which packets are routed by the attacker to its children to other distant nodes but does not transfer to its legitimate parent [6]. The main purpose of the intruder is to increase the latency by misdirecting the incoming messages due to which few packets are prevented from reaching the base station. The most popular Denial of Service Attack is the Misdirection attack. It changes the path of the packets in order create confusion among nodes.

Literature Review

Yogeesh Seralathan, et.al (2018) presented all the devices in the internet of things are controlled and connected with the help of internet [7]. Large number of sensitive data is being processed by the devices due to which the use of IoT devices increases widely. In order to large number of botnets, Malware like Mirai is widely used nowadays. This malware has been utilized in DDoS attacks as well in which every second up to 1.2 Terabytes of networks traffic is generated. They performed various experiments, in order to determine compromise done by an IoT device's in case of threat for the security and privacy of the data and they provide a case study of an IP camera. They also presented the importance of securing IoT and provide essential security practices for mitigating device exploitation.

Chalee Vorakulpipat, et.al (2018) presented the critical issue currently faced by the devices due large utilization of these devices. The major issue faced currently is the issue of the network security in the devices. The use of devices nowadays increased drastically in order to access the corporate networks due to which they are prone to the major security risks [8]. Due to these devices it is easy to access more channels for the corporate information. The need of the IoT security changes according to market needs as services of the IoT devices changes from time to time. They presented a concerns related to IoT security, reviews, and challenges faced by the devices as well as discussed the three generations of the IoT security.

Jesus Pacheco, et.al (2017) presented a framework for the security of IoT for the integration of a Smart Water Systems in the IoT, in a secure way. They also showed the procedure to use the threat model in order to protect or secure gateway which is the necessary part of the communication gateway. The functionality of this method is based on the concept that it utilizes a profile that is developed to accurately and characterizes the normal operations of gateway [9]. As per analysis, it is demonstrated that proposed approach of ABAIDS can detect both known and unknown attacks with high detection rates and low false positive alarms. They also have insignificant overhead in terms of memory and CPU usage. Proposed method protects the normal operation of the gateway in order to provide the availability.

Se-Ra Oh, et.al (2017) presented a connected, intelligent and context-aware device that works collectively known as internet of things (IoT). Security is the main consideration in the IoT devices as they are more vulnerable to attacks and directly affect the IoT device in the IoT platform [10]. In the interworking process, they are more prone to critical influence in all connected

IoT platforms. The security architecture of the oneM2M was discussed in this paper. Therefore, they developed an OAuth 2.0-based oneM2M security component in order to provide authentication and authorization which is necessary for the security of IoT and for the protection of interworking between IoT platforms.

U. M. Mbanaso, et.al (2017) presented a novel configurable policy-based specification and the threats and vulnerabilities faced by an IoT system were analyzed. In order to solve all the issues in multiple domains, these devices work collectively and smart entities have to more trusted, reliable and secure for the security and safety of end-to-end connectivity [11]. A mechanism was proposed by author in this paper by which all the IoT entities can express their capabilities and requirements. For the negotiation of provable attributes and resources they constructed a fine-grained policy mutually. In order to solve the dispute resolution and auditable, they provide a mechanisms which solve the issues such as trust, privacy and confidentiality in a unified manner. This method provides a greats success in the IoT environments.

Yiqun Zhang, et.al (2018) presented it a major challenge for the IoT devices to support different cryptographic algorithms and standards within the physical constraints. Author proposed a Recryptor in this paper which is a reconfigurable cryptographic processor which utilizes its computational capabilities in order to enhance the existing memory of a commercial general-purpose processor [12]. A 10-transistor bitcell supports, in-memory bitline computing for the support of different bitwise operations up to 512-bits wide. The programmability of the Recryptor's was demonstrated by implementing the cryptographic primitives of various public/ secret key cryptographies and hash functions. 6.8% average speedup and 12.8% average energy was achieved by Recryptor running at 28.8 MHz in 0.7 V as compared to software- and hardware.

Author Name	Year	Description	Outcome
Yogeesh Seralathan, Tae (Tom) Oh, Suyash Jadhav, Jonathan Myers, Jaehoon (Paul) Jeong, Young Ho Kim, and Jeong Neyo Kim	2018	In order to large number of botnets, Malware like Mirai is widely used nowadays. This malware has been utilized in DDoS attacks as well in which every second up to 1.2 Terabytes of networks traffic is generated.	They performed various experiments, in order to determine compromise done by an IoT device's in case of threat for the security and privacy of the data and they provide a case study of an IP camera.
Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Phithak Thaenkaew, Hoang Dang Hai	2018	The need of the IoT security changes according to market needs as services of the IoT devices changes from time to time.	They presented a concerns related to IoT security, reviews, and challenges faced by the devices as well as discussed the three generations of the IoT security.
Jesus Pacheco, Daniela Ibarra, Ashamsa Vijay, Salim Hariri	2017	The functionality of this method is based on the concept that it utilizes a profile that is developed to accurately and characterizes the normal operations of gateway.	Proposed method protects the normal operation of the gateway in order to provide the availability.
Se-Ra Oh, Young-Gab Kim	2017	In the interworking process, they are more prone to critical influence in all connected IoT platforms. The security architecture of the oneM2M was discussed in this paper.	They developed an OAuth 2.0-based oneM2M security component in order to provide authentication and authorization which is necessary for the security of IoT and for the protection of interworking between IoT platforms.
U. M. Mbanaso, G. A. Chukwudebe	2017	A mechanism was proposed by author in this paper by which all the IoT entities can express their capabilities and requirements.	This method provides a greats success in the IoT environments.
Yiqun Zhang, Li Xu, Qing Dong, Jingcheng Wang, David Blaauw, and Dennis Sylvester	2018	Author proposed a Recryptor in this paper which is a reconfigurable cryptographic processor which utilizes its computational capabilities in order to enhance the existing memory of a commercial general-purpose processor	6.8% average speedup and 12.8% average energy was achieved by Recryptor running at 28.8 MHz in 0.7 V as compared to software- and hardware.

Conclusion

The internet of things is the decentralized type of network in which sensor devices sense information and pass it to base station. The energy efficiency is the major issue of internet of things. The clustering is the approach which can improve lifetime of internet of things. In this review paper, various energy efficient approaches are reviewed in terms of certain parameters.

References

[1] Dongsik Jo and Gerard Jounghyun Kim, "ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", IEEE Transactions on Consumer Electronics, Vol. 62, Issue. 3, pp. 334-340, August 2016.

[2] Xinlie Wang, Jianqing Zhang, Eve. M. Schooler, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT", Communications (ICC), 2014 IEEE International Conference, vol. 19, issue 3, pp. 56-88, 2014.

[3] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Elsevier Future Generation Computer System, Vol. 29, issue 4, pp. 23-66, 2013.

[4] Mohamed Abomhara and Geir M. Koien, "Security and Privacy in the Internet of Things: Current Status and Open Issues", In Privacy and Security in Mobile Systems (PRISMS), pages 1–8, IEEE, vol. 7, issue 6, pp. 18-3, 2014

[5] Ahmad W Atamli and Andrew Martin, "Threat-Based Security Analysis for the Internet of Things", In Secure Internet of Things (SIoT), vol. 4, issue 1, pages 35–43, 2014.

[6] Luigi Atzori, Antonio Iera, and Giacomo Morabito, "The Internet of Things: A survey", Computer Networks, vol. 8, issue 6, pp. 18-30, 2010.

[7] Yogeesh Seralathan, Tae (Tom) Oh, Suyash Jadhav, Jonathan Myers, Jaehoon (Paul) Jeong, Young Ho Kim, and Jeong Neyo Kim, "IoT Security Vulnerability: A Case Study of a Web Camera", International Conference on Advanced Communications Technology(ICACT), IEEE, vol. 13, issue 9, pp. 16-30, 2018.

[8] Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Phithak Thaenkaew, Hoang Dang Hai, "Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study", International Conference on Advanced Communications Technology(ICACT), vol. 7, issue 4, pp. 14-33, 2018.

[9] Jesus Pacheco, Daniela Ibarra, Ashamsa Vijay, Salim Hariri, "IoT Security Framework for Smart Water System", 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications, IEEE, vol. 9, issue 3, pp. 11-30, 2017.

[10] Se-Ra Oh, Young-Gab Kim, "Development of IoT Security Component for Interoperability", IEEE, vol. 12, issue 4, pp. 67-89, 2017.

[11] U. M. Mbanaso, G. A. Chukwudebe, "Requirement Analysis of IoT Security in Distributed Systems", 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), IEEE, vol. 5, issue 7, pp. 20-30, 2017.

[12] Yiqun Zhang, Li Xu, Qing Dong, Jingcheng Wang, David Blaauw, and Dennis Sylvester, "Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor With In-Memory and Near-Memory Computing for IoT Security", IEEE JOURNAL OF SOLID-STATE CIRCUITS, vol. 9, issue 3, pp. 25-56, 2018.

