Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENERGY OVERHEAD EVALUATION OF SECURITY TRUST MODELS FOR IOT APPLICATIONS

[1]AMEER ALHASAN, [1]LUKMAN AUDAH, [2]AMJED ALABBAS

Wireless and Radio Science Centre (WARAS)
1Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia
86400 Parit Raja, Batu Pahat, Johor, Malaysia
2Department of Electrical and Computer Engineering Altinbas University
Muhmutbey Mahallesi, 34218 Bağcılar/ Istanbul, Turkey
E-mail: ameer.nadhum91@gmail.com, hanif@uthm.edu.my, amjad.razak@yahoo.com

ABSTRACT

Internet of things networks (IoT) has emerged as promising technology for handling small network based devices. However, its limited resources remain the main concern in implementing this type of networks. Energy one of the main factor of these resources where most of IoT devices depends on batteries. Energy reduction efforts are continuous in different trends; protocol overhead is one of the main topic in this direction. Most recently proposed trust-based security approaches include high overhead in term of energy consumption; however, this overhead is not investigated. In this paper, the energy overhead of recently proposed trust model research is investigated. Three of the main trust models for security purposed is investigated. Results show how protocol overhead can directly affect the energy consumption. It mainly demonstrates that high number of packets exchange in any algorithm can increase the energy overhead. Results shows that low communication overhead algorithm has efficiently reduced the power dissipation and enhance network lifetime

Keywords: *Internet Of Things (Iot) , Trust Model , Energy , Power Dissipation.*

1. INTRODUCTION

Recently, Internet of Things (IoT) has gradually became part of human lives due to the increasing access to wireless communication systems such as RFID, WiFi and 4G and the concept is multiple-folded [1]. It uses many services, standards and technologies. The data transfer from one node sensor to another in IoT devices is carried out through various communication architectures such as Machine-to-Machine (M2M) [2]. The first-hop path communication technology between IoT devices and server is usually made of wireless radio access for ease of deployment and installation [3].

There are many differences between IoT network characteristics that use wireless technologies and those that use traditional wireless or wired networks when the number of devices participating in one communication domain is huge [4]. Additionally, the quantity of generated traffic by IoT devices are mostly lower than those in traditional network devices. Because, each IoT device identifies and transmit a small packet of data to its corresponding IoT gateway [5]. Furthermore, IoT devices are limited in term of computing resources and battery and operate steadily for a longer period of time without human interference [6] [7].

The operation of IoT Devices depends principally on available sources of battery power [4]. So, the energy efficiency is one of the most critical task in management operations of IoT devices [8]. Various research works have been proposed to investigate energy efficacy for battery operated nodes and lifetime maximization [9]. Medium Access Control (MAC) protocols layer mainly focuses on specifying duty cycle of sensor nodes. On the other hand, data collection and several-to-one transmission is the main destination in routing layer protocols [4]. During deployment of IoT network, battery consumption should be considered as the major priority. On the other hand, the characteristics of IoT networks and its application are more complex when compared with the traditional WSNs in many perspectives. This include accurate use of wireless radio access technologies with IoT gateways, bidirectional traffic between the gateways and IoT devices and varied data for actuation and sensing [10].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

For this reason, energy consumption is a critical factor in implementation of any data communication approach in IoT networks [11]. Its practical applications in IoT are limited due to the high power consumption and limited bandwidth [12]. In this paper, the energy consumption of the recently proposed trust models of IoT gateways is measured. The remaining part of this paper is organized in the following sequence: in the first section, an overview of energy conservation issues are presented. Subsequently, the details of the investigated approaches are described. Thereafter, the evaluation, simulation parameters and topologies are described. Finally the simulation results are presented by describing the energy overhead of the investigated research works.

2. ENERGY CONSERVATION ISSUES IN IOT

Different factors affect energy conservation in IoT environment. For instance, issues of power saving in IoT devices during network realization of IoT/M2M is associated with the use of wireless radio technologies such as LTE-Advanced, Wi-Fi or Bluetooth devices [13]. On the other hand, IoT device activity has the highest impact on energy consumptions due to its critical role in reducing time IoT nodes remain in active status [14]. Some researchers inferred that collision can cause energy disputation in which Transmission process is repeated. Over hearing also is another problem caused by high density sensor nodes that can lead to interferences with neighbouring IoT devices during data transmission [15].

Nodes within reach exhibit a particular problem that leads to burn up of energy resources owing to the reception and processing unusable information. Protocols overhead is considered one of the main factors of power dissipation [16]. Also, IoT optimized protocols are expected to meet the requirement of IoT devices [17]. The protocols control and exchanged information depleted by the energy resources. The cost of data transmission is more than the cost of data processing [18]. However, data aggregation is required within clusters in other to minimize the amount of data transmitted, since cluster heads or Gateways are responsible for processing and monitoring queries [19]. It facilitates many energy dissipating effects [20].

In this process, data coming from different sources are combined into a single data packet which enables it to reduce redundancy and minimize number of transmissions [21]. Energy efficiency could be implemented in the proposed protocols through the use of a suitable metrics [22]. Different optimization process are required to minimize energy consumption overhead by minimizing communication and computation overhead and considering energy status of IoT devices in networks [16].

3. INVESTIGATION OF THE ENERGY OVERHEAD OF THE SECURITY TRUST MODEL

In this section, the communication and computation overhead of security-based trust model is measured. Three recent proposed research works are selected to investigate their performance. The papers are selected from recent related works in the field of trust based IoT security approaches. The proposed work on [23]. is a Trust-Based Adaptive Security in IoT (TAS-IoT) which depends mainly on providing security based trust model where IoT devices target traffic of its neighbours for security issues and the trust is calculated upon monitoring the results. The second proposed work in [24] is a Security & Trusted Devices under the Context of Internet of Things (STD-IoT). It focus mainly on the provision of security trust model where gateway monitor IoT devices that belongs to it and compute the trust based on its trust values. It then sent back information to the IoT devices as recommendations [25].

The third paper relies on design of Trust management system for Internet of Things which considers multiservice and context-aware approach (Context-IoT) [26]. This approach depends on trust manager that is responsible for investigation of the trustworthiness of each node in the network after the completion of each task and respond accordingly. When a network node is required to send data to a specific node, it first send a query packet to the trust manager inquiring for the trust of the destination and wait for the manager to response before it begins to communication with it.

4. PERFORMANCE METRICS

In this paper, energy is the main concern, thus the main evaluation metrics include average energy consumption, average energy remaining and the lowest energy remaining in the network node. NS2 simulator [27] provides an energy model for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

simulation of IoT and WSN devices. The Energy Model is a nodal attributed concept which represents the energy level in a mobile node [28].

Energy model is obtain using Class Energy Model in NS-2.35 with the following features:

- txPower: Transmission power in watts
- rxPower: Power Received in watts
- initialEnergy: Starting Energy in joules
- sleepPower : consumed energy in sleep status
- idlePower: consumed energy in idle state when where is no activities.

An update was implemented in the Energy Model of NS2 in other to add a sensor power that would indicate the amount of energy consumed during traffic monitoring.

Average consuming energy:

This evaluation metrics calculate the average value of the energy consumed in each IoT device. The energy consumed depends on the required communication overhead in term of sending, receiving and sensing activities of each node. The consumed energy of each node can be calculated using the following equation (1)

$$En_{Cons} = En_{Send} + En_{Rec} + En_{idle} + En_{sleep} + En_{Mon} \quad (1)$$

Where En_{Cons} : the consumed energy En_{Send},: energy consumed in sending data , En_{Rec} : is the energy consumed during data reception, En_{idle} is the energy consumed in an idle state of a device when no action is performed. En_{sleep} : Energy consumed by a node in a sleep state. En_{Mon} : The energy consumed when the node is monitoring or sensing data from other nodes

If a network contain N nodes, then the average consumed energy estimated using the equation (2) below:

$$En_{Cons\_Avg} \sum_{i=1}^{n} En_{Cons\_i}/n \quad (2)$$

Where En_{Cons_i} represent energy consumed at the node i.

Average remaining energy:

The average remaining energy indicate the average value of energy remained in the network nodes. It is an indication of the expected network lifetime. The remained energy can be estimated by subtracting the consumed energy from the initial energy as shown in equation (3) below.

$$En_{Rem} = En_{Init} - En_{Cons} \quad (3)$$

Where En_{Init} represents the initial nodal energy, En_{Cons} is the energy consumed at the node.

If a network contains N nodes, then the average consumed energy can be calculated using equation (4) below:

$$En_{Rem\_Avg} = \sum_{i=1}^{n} En_{Rem_i}/n \quad (4)$$

Note: All energy calculation used mill watt (mW) unit

5 SIMULATION TOPOLOGY

To assess the performance of the security, trust model, four different network topologies are designed to reflect a healthcare IoT device scenario. In this case, IoT devices are set to monitor health parameters such as Haemoglobin, Pulse blood pressure, Blood sugar and surveillance cameras. The scenario include 4 different rooms with each location comprising 10 IoT devices [29]. In the simulation scenario, a single room is increased at each simulation cycle, so that the number of nodes are varied from 10 to 40 nodes with each room comprising a single CH.

In the third scenario, each room is considered a trust manager. The network simulation topologies are shown in the Figure 1, Different number of nodes were used to investigate the energy consumption overhead in case of the different network nodes. Each of the 10 nodes have a cluster head. A constant bit rate traffic of 1mbps is transmitted from each node to other node [30].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

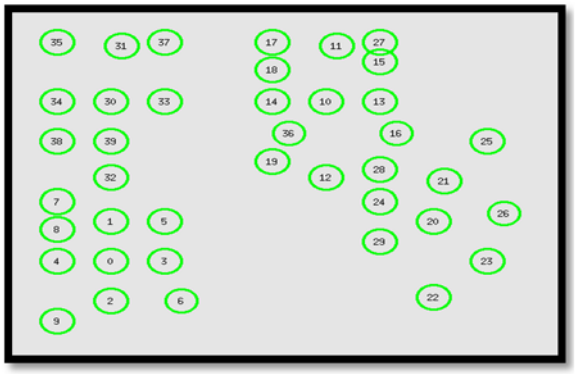

Figure 1: Simulation Topology Of 40 Nodes

The parameters used in the network simulation are assigned to the network nodes as listed in Table. Various scenarios are implemented in the simulation using different IoT devices. The three main implementation of the no trust model are TAS-IoT, STD-IoT and Context IoT.

As shown in Table 1, channel type used are wireless channel which connect all wireless nodes together in the simulation scenario for data exchange [31]. In this scenario, Radio-propagation model used is a two-ray-ground for long distance communication [32]. Network interface type used is wireless physical layer which deals with four important features of the network: electrical, mechanical, procedural and functional. Also, it defined the required hardware characteristics to be used for the data transmission such as signal strength, voltage/current levels, media and connector. Essentially, this layer ensures adequate reception of the bit sent on the other side of the network [33]. Omni antenna is the antenna type used to receive and transmit the signals in all directions. The antenna is suitable for most users due to their ability to provide reliable coverage over a large area and can accommodate multiple providers [34]. The MAC type is 802.11 NS-2 with its IEEE 802.11 support which are extensively used for simulation of wireless communication in research environment [35].

The topographical area was chosen to cover all units of clinics, big and small hospitals. The Routing protocol used is AODV and is designed for wireless and mobile ad hoc networks due to its flexibility and ability to allow nodes to enter and leave the network at will coupled with its limitation for node energy consumption [36]. The data flow used is a constant bit rate due to the fact that this scenario need to receive data at a constant bit rate like video data transfer to and from a digital video camera [37]. The packet size applied is 1000 bytes to enable transfer of video data with high quality. The data bit rate 1 mbps was selected to meet the requirements of camera traffic.

The main parameter considered for the trust model efficiency is the number of nodes. Because, the trust approach depends on the nodes to build the trust between nodes and provides security. This is followed by another factor that control the amount of data exchanged between the nodes [5]. This study considered majority of health care systems ranging from clinics to large hospitals. Therefore, the scenario used in this simulation includes 10, 20, 30, and 40 nodes to cover the vast majority of health care centre units. So, 10 nodes is for clinic, 20 nodes for small hospitals, 30 nodes for medium hospitals and 40 nodes for big hospital units. The simulation time is selected to meet the expected amount of consumed energy and the initial energy [38]. The management of the network topology is widely used as a mechanism to enhance wireless sensor networks lifespan (WSN), [39].

Table 1: Network values for the Simulation Parameters

PARAMETER	VALUE
Channel type	Wireless Channel
Radio-propagation model	Two Ray Ground
Type of Network Interface	Wireless Phy
Antenna type	Omni Antenna
Interface queue type	DropTail/PriQueue
Maximum packet in Queue	50
MAC type	802_11
Topographical Area	1000 x 1000 sq.m
Routing protocols	AODV
Number of IoT nodes	10,20,30,40
Simulation Time	100 seconds
Data Flow	CBR
Packet Size	1000 byte

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Data Bit rate	1 mbps
Initial Energy	1000 Joule
RX Power	1.0
TX Power	1.0
Sleep Power	0.1
Transition Power	0.2
Idle Power	0.5

6 RESULTS

As illustrated earlier, four main scenarios are applied: no security trust model, TAS-IoT model STD-IoT and context-IoT model. Figure **2**, illustrates the results of the evaluation metrics when no security trust model is applied. The x-axis illustrates the number of nodes in the topology and y-axis is the number of nodes. The amount of consumed energy is quite small with an average value of 46 mW, the remaining energy is about 953 mW, which indicate that only about 4% of the initial energy is consumed during the simulation period, and the minimum level of energy for the highest consuming node is 900 mW.

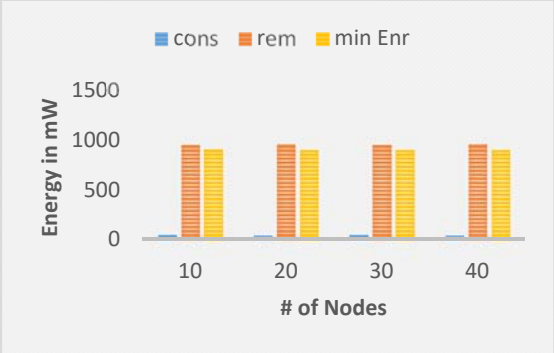

Figure 2: Evaluation Metrics Of No Trust Scenario

In Figure 3: the evaluation metrics for TAS-IoT Model is presented. It shows the average consumed energy of about 240 mW, the average remaining energy of 759 mW, this indicates that the average energy consumed is 24% of the initial nodes energy. While, the lowest energy level in the node is 373 mW.

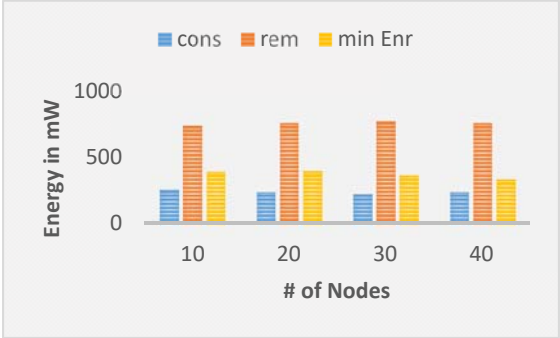

Figure 3: Evaluation Metrics Of Tas-Iot Model Scenario

The evaluation metrics results of STD-IoT model is shown in Figure 4 with the average consumed energy of about 157 mW, the average remaining energy is 842 mW, however, if the cluster gateway energy is ignored, and the minimum remaining level of nodes energy is about 790 mW. Therefore, the result shows that the average consumed energy is about 16% of the initial node energy.

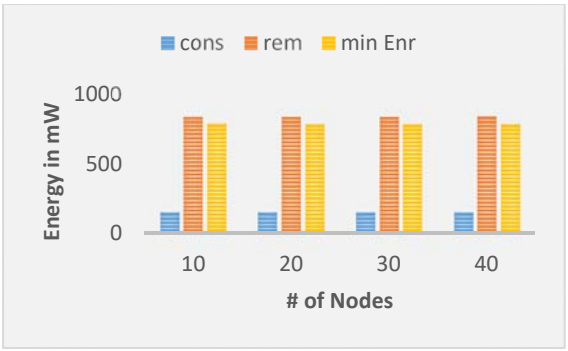

Figure 4: The Evaluation Metrics Of Std-Iot Model Scenario

Figure. 5, shows the third mechanism (context-IoT) with an average consumed energy of about 531mW, which implies that dramatic decrease in energy consumption is observed. The figure also shows that the remaining energy is declined abruptly when the average remaining energy is about 469 mW, and the minimum level of energy for the least node has dropped to zero level when some nodes are depleted completely.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

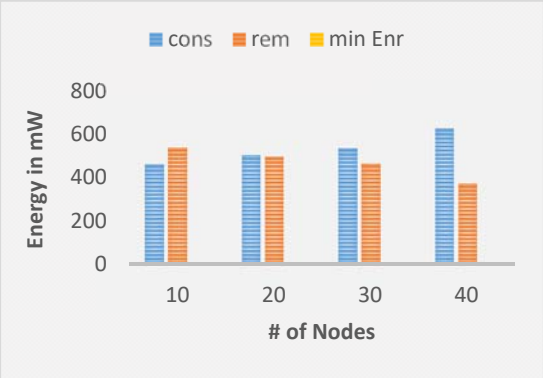

Figure. 5. Evaluation Metrics Of CONTEXT-Iot Model Scenario

7 RESULTS COMPARISON

Figure 6 illustrates energy consumption result for the four scenarios: no trust model TAS-IoT, SAD-IoT and CONTEXT-IoT models. The result indicates that the amount of energy consumed is increased from the initial energy of 4 % in no trust model to 25% when TAS-IoT model is applied. This occurred when all network node are working on the monitoring mode to investigate data delivery. On the other hand, when the monitoring task is directed to the cluster IoT gateway, the energy consumption is decreased downwards to 16% when SAD-IoT is implemented due to the recommendation system of the IoT gateway in the IoT device nodes.

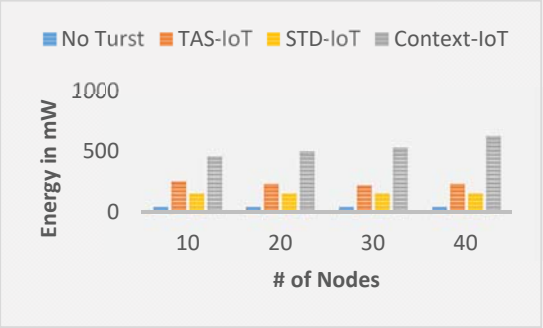

Figure. 6. Consumed Energy For The Four Main Scenarios

The result of the remaining energy levels for the four scenarios: no trust model, TAS-IoT SAD-IoT, and CONTEXT-IoT models is shown in Fig. 7, The result shows that the amount of remaining energy is decreased from the initial energy of 95 % in no trust model to 76% when TAS-IoT model is applied, where all network node is working on the monitoring mode to investigate the data delivery and existence of any security risk. On the other hand, when the monitoring task is directed to the cluster IoT gateway, the remaining energy level is increased up to 84% when SAD-IoT is implemented due to the recommendation system of IoT gateway to IoT device nodes. The remaining energy in the CONTEXT-IoT goes down abruptly due to excessive data communication to achieve reliable trust level among nodes using the trust manager. The result shows that STD-IoT outperformed the CONTEXT –IoT with about 79% in energy conservation.

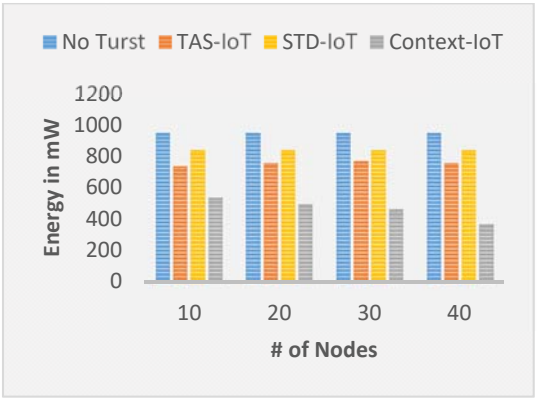

Figure 7: Remaining Energy For The Four Main Scenarios

The minimum node remaining energy for the four simulated scenarios are shown in Figure 8 the remaining value is varied depending on the used scenarios for different nodes numbers. When no trust model is applied, the remaining average energy level is 902 mW, however, it decreased to 790 mW, and When STD-IoT is applied. This means that it decreases to 12% of the value in no trust scenario. On the other hand, when TAS-IoT mode is applied, it reduced to 373 mW, which indicate a decrease by 58% of the value in no trust scenario and 53% of the value of SAD-IoT trust. Finally, the CONTEXT-IoT exhibited the lowest node energy when it is completely exhausted at the nodes with a remaining energy of zero.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

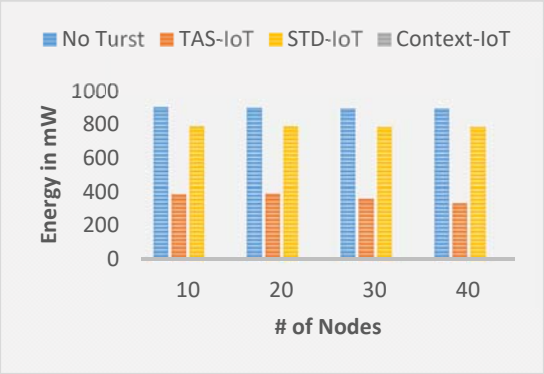

Figure 8: The Minimum Remaining Node Energy For The Four Main Scenarios

8 CONCLUSION

Summarily, the result shows that implementation of security trust model increases energy consumption due to the communication and computation overhead. The result also shows that CONTEXT-IoT mechanism consumed the highest amount of energy when huge number of data transmission is carried out to build trust and query for trust values. This is because CONTEXT-IoT mainly depends on trust manager which is responsible for assessing the trustworthy of each node in the network after the completion of each task and act.

Therefore, when a network node needs to send data to a specific node, it first sends a query packet to the trust manager demanding for the trust of the destination and wait for the manager's response before it begins to communicate with it. On the other hand, TAS-IoT consume a smaller amount of energy than the CONTEXT-IoT when building or distributing trust values to the network members. Because, it depends mainly on provision of security-based trust model by enabling IoT devices to sense its neighbour's traffic in terms of security issues and the trust is calculated upon monitoring results. So, the best performance in terms of energy consumption is achieved by STD-IoT due to its fewer data exchanged requirement to build and maintain trust level. The security trust model of STD-IoT depends on gateway monitoring of the IoT devices within it domain. The trust value is finally sent to IoT devices as recommendations. Hence, the STD-IoT has outperformed the context–IoT with about 79% and TAS-IoT with about 53% in terms of energy conservation.

9 IMPLICATION & RECOMMENDATION

The aim of this study is to investigation how security trust model effect on energy node in the internet of things network, the result reveals that when the security complexity increases that leads to high energy consumption [which directly impacts on efficiency and quality of service for these nodes. The findings of the current study can be beneficial for researchers as it can show them the link between the security complications and energy consumption. in this study recommendation to the researchers whom are interested in the field of designing a trust model in internet on things network to considering energy node trust as a main factor in term of designing trust model to enhancing the reliability, integrity, and quality of service.

REFERENCES

[1] Orsino A, Araniti G, Militano L, Alonso-Zarate J, Molinaro A, Iera A. Energy efficient IoT data collection in smart cities exploiting D2D communications. Sensors. 2016;16(6):836.

[2] Beevi MJ. A fair survey on Internet of Things (IoT). In2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS) 2016 Feb 24 (pp. 1-6). IEEE.

[3] Čolaković A, Hadžialić M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks. 2018 Oct 24;144:17-39.

[4] Kaur N, Sood SK. An energy-efficient architecture for the Internet of Things (IoT). IEEE Systems Journal. 2015 Oct 7;11(2):796-805.

[5] Sharma V, You I, Andersson K, Palmieri F, Rehmani MH. Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey. arXiv preprint arXiv:1903.05362. 2019 Mar 13.

[6] Ketema G, Hoebeke J, Moerman I, Demeester P, Tao LS, Jara AJ. Efficiently observing Internet of Things resources. In2012 IEEE International Conference on Green Computing and Communications 2012 Nov 20 (pp. 446-449). IEEE.

[7] Samie F, Tsoutsouras V, Bauer L, Xydis S, Soudris D, Henkel J. Computation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

offloading and resource allocation for low-power IoT edge devices. In2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) 2016 Dec 12 (pp. 7-12). IEEE.

[8] Kim M, Park S, Lee W. A Robust Energy Saving Data Dissemination Protocol for IoT-WSNs. KSII Transactions on Internet & Information Systems. 2018 Dec 1;12(12).

[9] J. SathishKumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, 2014.

[10] Abedin SF, Alam MG, Haw R, Hong CS. A system model for energy efficient green-IoT network. In2015 International Conference on Information Networking (ICOIN) 2015 Jan 12 (pp. 177-182). IEEE.

[11] Baker T, Asim M, Tawfik H, Aldawsari B, Buyya R. An energy-aware service composition algorithm for multiple cloud-based IoT applications. Journal of Network and Computer Applications. 2017 Jul 1;89:96-108.

[12] Luan S, Bao J, Liu C, Li J, Zhu D. Power Saving Scheme by Distinguishing Traffic Patterns for Event-Driven IoT Applications. KSII Transactions on Internet & Information Systems. 2019 Mar 1;13(3).

[13] Van Kranenburg R, Bassi A. IoT challenges. Communications in Mobile Computing. 2012 Dec 1;1(1):9.

[14] Abbas Z, Yoon W. A survey on energy conserving mechanisms for the internet of things: Wireless networking aspects. Sensors. 2015 Oct;15(10):24818-47.

[15] Mössinger M, Petschkuhn B, Bauer J, Staudemeyer RC, Wójcik M, Pöhls HC. Towards quantifying the cost of a secure IoT: Overhead and energy consumption of ECC signatures on an ARM-based device. In2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2016 Jun 21 (pp. 1-6). IEEE.

[16] Santiago S, Arockiam L. Energy Efficiency in Internet of Things: An Overview. International Journal of Recent Trends in Engineering & Research (IJRTER). 2016 Jun;2(6):475-82.

[17] Tozlu S, Senel M, Mao W, Keshavarzian A. Wi-Fi enabled sensors for internet of things: A practical approach. IEEE Communications Magazine. 2012 Jun 6;50(6):134-43.

[18] Alhasan A, Audah L, Alhadithi OS, Alwan MH. Quality of Service Mechanisms in Internet of Things: A Comprehensive Survey. Journal of Advanced Research in Dynamic and Control Systems. 2019;11(02-Special Issue):858-75.

[19] Minoli D, Sohraby K, Occhiogrosso B. IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems. IEEE Internet of Things Journal. 2017 Jan 4;4(1):269-83.

[20] Al-Shammari HQ, Lawey A, El-Gorashi T, Elmirghani JM. Energy efficient service embedding in IoT networks. In2018 27th Wireless and Optical Communication Conference (WOCC) 2018 Apr 30 (pp. 1-5). IEEE.

[21] Lin H, Bergmann N. IoT privacy and security challenges for smart home environments. Information. 2016 Sep;7(3):44.

[22] Wang K, Wang Y, Sun Y, Guo S, Wu J. Green industrial Internet of Things architecture: An energy-efficient perspective. IEEE Communications Magazine. 2016 Dec 16;54(12):48-54.

[23] Hellaoui H, Bouabdallah A, Koudil M. Tas-iot: trust-based adaptive security in the iot. In2016 IEEE 41st Conference on Local Computer Networks (LCN) 2016 Nov 7 (pp. 599-602). IEEE.

[24] Sklavos N, Zaharakis ID, Kameas A, Kalapodi A. Security & trusted devices in the context of internet of things (IoT). In2017 Euromicro Conference on Digital System Design (DSD) 2017 Aug 30 (pp. 502-509). IEEE.

[25] Bedi G, Venayagamoorthy GK, Singh R, Brooks RR, Wang KC. Review of internet of things (IoT) in electric power and energy systems. IEEE Internet of Things Journal. 2018 Feb 5;5(2):847-70.

[26] Saied YB, Olivereau A, Zeghlache D, Laurent M. Trust management system design for the Internet of Things: A context-aware and multi-service approach. Computers & Security. 2013 Nov 1;39:351-65.

[27] Gautam G, Sen B. Design and simulation of wireless sensor network in NS2. International Journal of Computer Applications. 2015 Jan 1;113(16).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[28] Zhou HY, Luo DY, Gao Y, Zuo DC. Modeling of node energy consumption for wireless sensor networks. Wireless Sensor Network. 2011 Jan 30;3(01):18.

[29] Rghioui A, L'aarje A, Elouaai F, Bouhorma M. The internet of things for healthcare monitoring: security review and proposed solution. In2014 Third IEEE International Colloquium in Information Science and Technology (CIST) 2014 Oct 20 (pp. 384-389). IEEE.

[30] Catarinucci L, De Donno D, Mainetti L, Palano L, Patrono L, Stefanizzi ML, Tarricone L. An IoT-aware architecture for smart healthcare systems. IEEE Internet of Things Journal. 2015 Mar 27;2(6):515-26.

[31] Nayyar A, Singh R. A comprehensive review of simulation tools for wireless sensor networks (WSNs). Journal of Wireless Networking and Communications. 2015;5(1):19-47.

[32] Eltahir IK. The impact of different radio propagation models for mobile ad hoc networks (MANET) in urban area environment. InThe 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 2007 Aug 27 (pp. 30-30). IEEE.

[33] Radhakrishnan R, Edmonson WW, Afghah F, Rodriguez-Osorio RM, Pinto F, Burleigh SC. Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view. IEEE Communications Surveys & Tutorials. 2016 May 9;18(4):2442-73.

[34] Gao F, Ma H, Gao P, Jiang Y, He J, Zhu W, Liu X, Zhang D, inventors; CHINA MOBILE GROUP DESIGN INSTITUTE CO., LTD., assignee. Broadband dual-polarized omni-directional antenna and feeding method using the same. United States patent US 9,209,526. 2015 Dec 8.

[35] Chen Q, Schmidt-Eisenlohr F, Jiang D, Torrent-Moreno M, Delgrossi L, Hartenstein H. Overhaul of IEEE 802.11 modeling and simulation in ns-2. InProceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems 2007 Oct 23 (pp. 159-168). ACM.

[36] Kim JM, Jang JW. AODV based energy efficient routing protocol for maximum lifetime in MANET. InAdvanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06) 2006 Feb 19 (pp. 77-77). IEEE.

[37] Lu J, Jiang W, Wallace G, inventors; Apple Inc, assignee. Single pass constrained constant bit-rate encoding. United States patent application US 11/108,157. 2006 Oct 19.

[38] D'Angelo G, Ferretti S, Ghini V. Multi-level simulation of internet of things on smart territories. Simulation Modelling Practice and Theory. 2017 Apr 1;73:3-21.

[39] J. Aparicio, J. J. Echevarria, and J. Legarda, "A software define d networking approach to improve the energy efficiency of Mobile Wireless sensor Network