Journal of Engineering Science and Technology
Vol. 16, No. 2 (2021) 968 - 987

AN ENERGY AWARE QOS TRUST MODEL FOR ENERGY CONSUMPTION ENHANCEMENT BASED ON CLUSTERS FOR IOT NETWORKS

AMEER ALHASAN[1,*], LUKMAN AUDAH[1],
MOHAMMED HASAN ALWAN[2], O. R. ALOBAIDI[3]

[1]Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia
86400 Parit Raja, Batu Pahat, Johor, Malaysia
[2]Department of Communication, College of Engineering,
University of Diyala, Baqubah, Iraq
[3]Department of Electrical Electronic & Systems Engineering, Faculty of Engineering & Built Environment, University Kebangsaan Malaysia (UKM),43600 Bangi, Selangor, Malaysia
*Corresponding Author: ameer.nadhum91@gmail.com

Abstract

Given the prevalence of IoT applications which caused various research issues one of the important is the energy consumption of IoT devices. Therefore, it is necessary to define a suitable and reliable service model that can meet the requirement of IoT applications and handle the levels of quality of services. Minimization of energy consumption are continuously being researched, and protocol communication has been identified as one of the major causes of increasing power consumption. In this paper, Quality of Service (QoS) approach to IoT application based on energy-aware trust model is proposed which includes four parameters such as communication trust, dependability trust, delay trust, and energy trust. These parameters are built for four different scenarios by using the k-mean clustering algorithm, the final trust for each node will calculate, and nodes will classify based on the level of trust. The results show that the proposed service model has lower communication overhead and, thus, smaller energy consumption amount is achieved when compared with recently proposed models. The proposed approach decreases the energy consumed up to about 50% than the Context-IoT approach and 43% than Security & Trusted Devices (STD-IoT) approach.

Keywords: Clustering, Energy aware, Internet of Things, K-mean, Trust model Quality of Service

1. Introduction

The Internet of Things (IoT) is a domain in several academic disciplines that covers several topics from purely technical issues, including semantic queries and routing protocols, to a combination of technical and social issues like usability, security, and privacy, in addition to the business domain [1]. Physical objects' virtual image is provided by IoT technology through the internet connection. Modern advancement in networking software and hardware such as Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN) have been crucial in enhancing IoT technology [2]. IoT is a concept that involves different objects and communication mechanism for data exchange between smart devices. Recently, the term IoT is more of a description of a vision where every device can connect to the Internet and exchange data. IoT is considered fundamental in the future, where it brings up opportunities for various innovations and new services [3]. Energy consumption is an essential factor that we should consider when designing a trust-model for IoT networks [4]. All devices can connect to a single network and communicate with each other. These devices can work in an unguarded and widely spread environments which can eventually lead to major QoS and security challenges [5]. The heterogeneous nature of IoT networks requires new demands for trust the process of data exchange and computation trust among different network nodes is a complicated problem due to the limited resource of IoT devices [6]. More computation and communication require higher computation and energy resources, which are not available for various IoT devices [7]. In particular, the mechanism of the trust management in various nodes networks should follow similar criteria, either subjective or objective [8].

IoT presents various Quality of Service (QoS) requirements which does not exist in conventional homogeneous wireless and wired networks [9]. A built-in QoS guarantees are required to provide a reliable end-to-end intelligent system that meets the requirement of a complete acquisition transmission interpretation action loop. Therefore, different network mechanisms and protocols need to be developed for IoT. QoS is considered as one of the most critical networking issues that have obtained researchers substantial attention for both wired and wireless networks [10]. QoS is one of the leading research concerns in the field of IoT networks. However, the limitation of resources of IoT devices is considered as one of the main obstacles against developing a reliable QoS handling mechanism [11]. Interactions and data exchange between IoT devices can provide a reliable trust model where the QoS approach can be built upon [12].

Different approaches have been proposed to design the trust model most of these proposed mechanisms mainly provide security for IoT networks [13]. Based on state of the art, there is a lack of study for build trust model by considering QoS trust and energy consumption. However, the trust model can be built to focus on QoS parameters, including throughput, delay, packet loss, and energy consumption. Scalability is also one of the main problems present in IoT networks that consist of a high number of devices [14]. The main contribution of this paper is the design of an energy aware QoS trust model for IoT healthcare devices, that considers energy and QoS in building trust relation and reduce the energy consumption significantly, when updating the trust values between network members. Furthermore, this study could be effective for researchers who interested in developing IoT devices in the healthcare system.

The remaining part of this paper is organized as follows: Section 2 discusses the literature review of recent trust models proposed for IoT networks using different approaches and mechanisms. Section 3 describes the details of the energy-aware trust model for handling QoS between IoT devices, the details of trust calculation and updating mechanism to reduce energy consumption. The simulation model used to evaluate performance is then described in Section 4 before the results are presented in Section 5. Finally, conclusions and future research directions are provided in Section 6.

2. Literature Review

To achieve IoT network trust data transmission, and communication trust play an essential and critical role in gaining IoT network trust. Recent enhancements in data wireless networking and communications can be employed to achieve Data communication trust. Indeed, the IoT networking and communication protocols trustworthy has to support the heterogeneous and specific context of IoT network that generate new performance challenges and issues. Some of the related existing works are presented below.

TRM-IoT model proposed by Chen et al. [15] a generalized and unified mechanism was introduced to handle the issue of trust and reputation by utilizing the development of sensor nodes community in the Wireless Sensors Network (WSN) of IoT in Cyber-Physical Systems. Furthermore, the proposed mechanism has been introduced for Cyber-Physical Systems (CPS) an authentication mechanism is also included. However, QoS approach is not considered where the primary purpose is to deliver secure data delivery for all types of data in the same manner where high and low priority are handled in the same way. Bao and Chen [16] proposed a scalable trust management protocol for IoT. It emphasizes mainly on the social relationships between nodes. Multiple trust properties are considered, including community-interest to account, cooperativeness, and honesty for social interaction. The proposed mechanism depends on social relationships where power consumption is not included in trust parameters. All traffic is handled in the same manner with low and high priority exchanged similarly.

Trustworthy infrastructure services for a secured and privacy respected IoT was proposed by Gessner et al. [17] protect data of users is essential, and interests, the privacy of users, and confidentiality of data must be guaranteed. Moreover, each request and response in the structure of IoT has to be authenticated suitably and securely to assure responsibility and convenient operation. Xu et al. [18] proposed an architecture of trustable agent and agency. In this regard, a hardware chip, referred to as Trustworthy Agent Execution Chip (TAEC), is installed on each IoT node to provide an autonomic, trusted hardware execution environment for different network agents.

The study by Ning et al. [19] used the Unit and Ubiquitous IoT (U2IoT) to address the cybersecurity issues. The security approaches are recommended depending on the activity cycle of cyber-entity. Then a secure interaction solution is established for different interaction scenarios with both privacy and security considerations. The proposed mechanism does not consider various trust issues like trust relations and decision, and QoS. Also, all proposed mechanism does not acknowledge traffic classes and priority where traffic type is not considered in trust

metrics and all data types are handled in the same manner. A context-aware and multi-service trust management system for the IoT was proposed by Saied et al. [20] the approach clarification aims to manage collaboration in a nonhomogeneous IoT structure encompass nodes with various resource abilities. To create an association, support, and practicability of trusted elements in a group of cooperating services. A single point of failure approach has been used where trust manager failure can result in network trust model failure. Also, higher communication overhead and long computation are assumed in the bootstrapping period. QoS is also not considered in building the trust model.

A trust management monitoring technique is established based on structural modelling of loT proposed by Gu et al. [21] The loT is decomposed into three layers: application layer, a core layer, and sensor layer, from sides of the network structure of loT. Trust management for a special purpose for each layer is controlled accordingly, and these purposes include self-organized, effective routing, and multi-service one by one. The proposed mechanism introduced a high computation overhead in different layers to build and support the trust model, where IoT limited node resources can be exhausted. In this case, QoS is also not considered where all data are handled similarly.

Chen et al. [22] proposed and analysed design adaptive trust management notions for social IoT systems where social relationships include changes among the IoT device owners. The design trade-off is revealed between trust convergences against the trust fluctuation in the design of the adaptive trust management protocol. Alternatively, work by Chen et al. [23] extends this model by adding comprehensive simulation effectiveness, assess state-of-the-art related work. In light of this, a more advanced attacker model for analysing the flexibility against these attacks arranges smart storage management planning for the ability to limit IoT devices. It is due to scalability with a comprehensive evaluation, addressing the best way to merge social similarity metrics to evaluate rates for application performance maximization. The proposed mechanism targets social networks and services. Also, data priority was not included in the trust management, where all data are handled similarly.

A novel IoT trust and reputation model was proposed by Asiri and Miri [24] employs distributed probabilistic neural networks (PNNs) to cluster trustworthy IoT devices from malicious nodes. In addition, it outfits the problem of the cold start in IoT networks by expecting ratings for newly joined nodes depending on their characteristics and information collected over time. The processing task is wholly distributed. Proposed model trying to conquer limitations of other trust models by training the eventuality neural network and adapt its weights count on 'nodes' resemblance and the quality of data which is sent.

Based on the state of art trust models and control approaches, most of these approaches are designed for a specific purpose environment. The emphasis is made more on Security issues about applying a reliable trust model to prevent attacks. Other than that, approaches introducing higher communication and processing overhead to building the trust model and exchange trust parameters reliant on a specific environment are discussed. However, there is an identifiable gap in the studies for QoS, and different priority traffic handling approaches, that are not introduced as required metrics in building a trust model. Moreover, energy

consumption needs to be considered in term of trust model designing for IoT devices as a fundamental factor due to its potentialities of effecting on the efficiency of these devices.

3. QoS-Energy Aware Trust Model

An energy aware QoS model was proposed for IoT environments; the trust model was built considering different communication factors related to data communication includes communication trust, dependability trust, delay trust and energy trust. Other factors also include energy consumption and remaining energy as well. Heterogeneous traffic requires different classes of services to meet with the requirements of each flow higher priority traffic requires better handling mechanism in terms of higher throughput and packet delivery ratio and lower delay. Therefore, these classes of services are defined depending on the trust level estimated in the calculating trust phase. The proposed mechanism can exhibit enhanced performance when implementing QoS in the IoT where communication and computation overhead is minimized, particularly in a limited resources environment.

Furthermore, the whole framework is demonstrated in Fig. 1. The trust of IoT cluster members is calculated based on four different trust values on the data query phase. Based on these values, these members are clustered into a different number of clusters using the K-means algorithm, and members then send data based on the clustering results. The member of each group is then updated based on the updating results of the data query process and if one of any cluster members is transferred from a cluster to another one. All members are updated about the new member cluster.

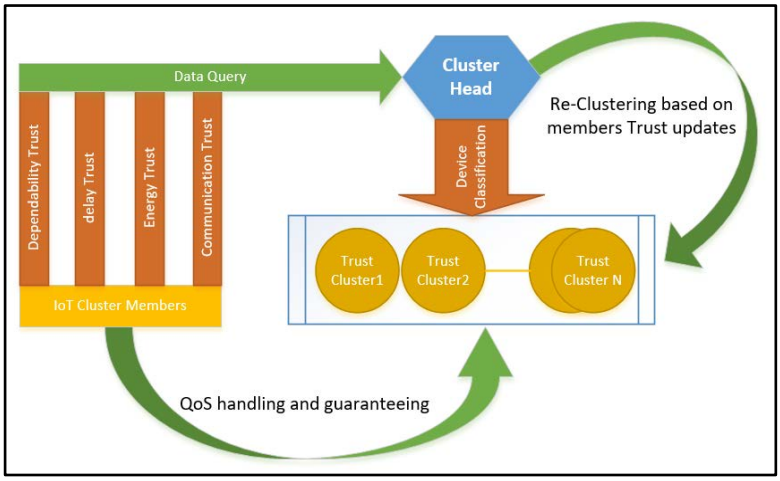

Fig. 1. The architecture of the energy aware trust model.

3.1. Trust level computation

The trust levels among IoT devices of the IoT networks are computed using a trust model based on well-defined metrics. Trusting confirmation events for the trust model will be defined to update the trust levels of IoT nodes. Trust model metrics can be defined to meet the behaviour of IoT devices.

Different research directions have been proposed to define and built trust module metrics that provide a combination of both social trust and quality of service concepts [25, 26]. When selecting a reliable trust metrics, performance, and security requirements are considered beside the ability to be a single IoT device of one or more groups or clusters at the same time. Defined trust metrics should consider both direct IoT device observations and their reputation in other clusters or groups.

The proposed trust model considers both node energy and QoS parameters as fundamental parameters in building the trust model. Devices involved in the IoT network are divided into clusters to maintain the network scalability. For each network cluster, a cluster head is selected depending on the energy levels, which is more likely an IoT device that is connected to a power source. Clustering IoT devices provide efficient solutions for scalability where dense IoT networks can be adequately handled.

The trust model of proposed mechanism mainly calculates a final trust value as shown in Eq. (1). which is defined in term of four main values: Communication trust (CT), dependability trust (DT), delay trust (PT), and Energy trust (ET). during a predefine time duration, where.

$$T_{Final} = (CT, PT, DT, ET) \tag{1}$$

A cluster head maintains a matrix for all devices belong to its cluster as shown below in Eq. (2).

$$T = \begin{bmatrix} C_{T,1} & P_{T,1} & D_{T,1} & E_{T,1} \\ C_{T,2} & P_{T,2} & D_{T,2} & E_{T,2} \\ C_{T,m} & P_{T,m} & D_{T,m} & E_{T,m} \end{bmatrix} \tag{2}$$

Data trust is calculated in terms of different parameters, including transmission rate, packet dropping rate, successful delivery rate, and delay. Moreover, energy trust is calculated in terms of power-consuming rate over time and remaining energy levels. The proposed approach includes four main phases, as shown in Fig. 2.

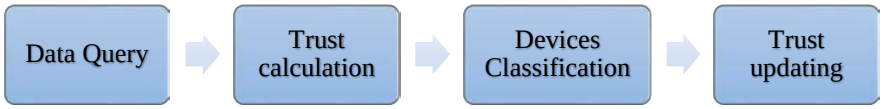

Fig. 2. energy aware-IoT trust model phases.

3.2. Data query

The trust of a cluster member is maintained by the cluster head. Any trust update at the cluster member is provided to the cluster head. Consequently, cluster head collect these values based on the cluster 'members' feedback. When the trust values are changed with an amount more than a threshold, the cluster head re-initiates the trust clustering and assigns the cluster member to the new QoS clusters while informing all the cluster members. Each cluster member maintains a data trust evaluation parameter for communication with his neighbour, a value between 0 to 1 is assigned to neighbour communication sessions during a predefined period of time β. These parameters include trust parameters, which are communication trust, dependability trust, delay trust, and energy trust.

3.3. Trust level calculation

The final trust is cumulative of data trust and energy trust. Data trust includes communication, dependability, and delay trust. The communication trust is represented in terms of link utilization, which can be calculated using the following Eq. (3). Where is Tx_{β} is the transmission data.

$$C_{T,\beta} = \frac{Tx_{\beta}}{Link\ Bandwidth} \tag{3}$$

The PT is measured in terms of successful and unsuccessful data delivery attempts, as defined in [27]. This is calculated as shown below in Eq. (4).

$$P_{T,\beta} = \frac{1}{K} \sum_{i=0}^{K} \left(\frac{S_{\beta}}{S_{\beta}+F_{\beta}}\right)\left(\frac{1}{\sqrt{F_{\beta}}}\right) \tag{4}$$

Where S_{β} , is the number of successful transmissions, F_{β} is the number of failed transmission and k is the number of packets send by each node because the DT refer to successful transection comparing with failed transection.

The DT can be estimated by the average delay of the successful transaction during the period of time β as shown below in Eq. (5). Where the E2E delay is the end-to-end delay.

$$D_{T,\beta} = \frac{1}{K \sum_{i=0}^{k} E2E\ Delay} \tag{5}$$

Devices communication trust and energy trust parameters are retrieved by cluster head, which includes communication trust calculated parameters and remaining energy. Cluster head specifies the duration time depending on the remaining energy level, where longer time is used with a lower energy level. For energy trust calculation, when node energy information is retrieved that includes remaining energy, the CH maintained the time of the received data, the consuming rate is then calculated as in Eq. (6) and (7).

$$Enr_{cons\ (t0,t1)} = \frac{Enr_{rem,t0} - Enr_{rem,t1}}{t_1 - t_0} \tag{6}$$

Where $Enr_{rem,t0}$ is the remaining energy at time t_0, $Enr_{rem,t1}$ is the remaining energy at time t_1 depending on this consumed energy during period of time $\beta = t_1 - t_0$ which can be defined as shorter or longer based on network analysis scenarios. The $C_{T,\beta}$ for a window time duration of t value can be defined as follow:

$$C_{T,\beta} = \frac{Enr_{rem,t1}}{Enr_{cons,\beta}} \tag{7}$$

3.4. Devices classification

Devices in a cluster are then classified to provide capabilities of providing different levels of QoS. These levels depend mainly on the calculated trust level. A higher trust level offers a broader range of QoS classes where data delivery can be guaranteed. However, a lower trust level indicates lower QoS guarantee features. In this phase, the decision depends on the priority of data being sent. Four different data priority classes for providing different levels of QoS can be defined.

Depending on the device quality level, which can be achieved and represented in terms of collected sent. Devices are classified into four main clusters depending on the final trust value: Q1 to Q4. Where Q4 includes the highest trustworthy for QoS delivery, and Q1 includes the lowest trustworthy and QoS levels.

K-means clustering algorithm is used to classify devices to the closest class of the four main classes. K-means is a very lightweight and efficient clustering algorithm, particularly in the case of a predefined number of clusters and predefines cluster centroids. K-means calculates the distance between the existing IoT devices parameters depending on the collected trust parameters retrieved for the corresponding IoT device. The Euclidean distance between the recently added IoT devices and the predefined four cluster centroids members are calculated using the following Eq. (8).

$$Distance_{D1,D2} = \sqrt[2]{\left(C_{T,1} - C_{T,2}\right)^2 + \left(P_{T,1} - P_{T,2}\right)^2 + \left(D_{T,1} - D_{T,2}\right)^2 + \left(E_{T,1} - E_{T,2}\right)^2} \quad (8)$$

where D1, D2 represents the comparing devices, the number of clusters is set to four different clusters to provide 4 levels of traffic classes. Clusters centroids are set to 0.2, 0.4, 0.6, and 0.8 corresponding to the centroids of the clusters to minimize the calculation overhead. This depends on the approach of using similar devices are clustered into a single cluster depending on the estimated cluster level. Fig. 3. illustrates the device classification step when a new device is enrolled into an existing network. The distance between the device trust level and the existing clusters member is calculated, and the new device is clustered using K-means into one of these clusters.

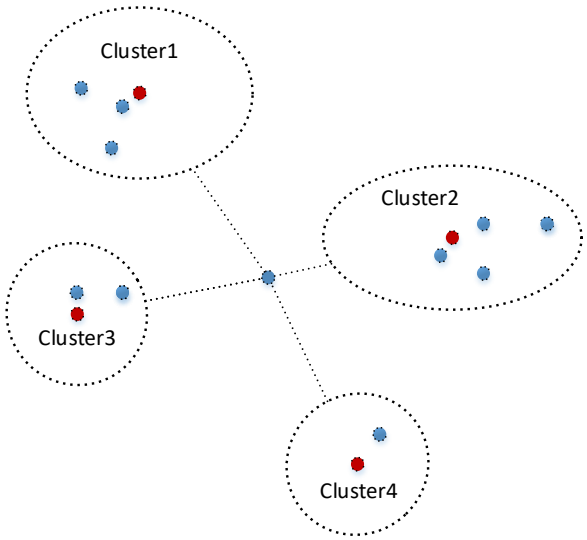

Fig. 3. IoT Devices classification using K-means.

Lastly, when data is required to be transmitted, the cluster of the destination device is retrieved according to the data priority.

3.5. Trust updating

Network dynamicity is reflected on the trust level of each node where the trust parameters are updated after each transaction. Updated parameters are forwarded to the CH periodically depending on time period β. CH maintains the trust level of all of the devices belonging to that cluster Device classification is performed in a periodic manner depending on the network status. If the network is busy, it is updated more frequently. Furthermore, if the recently gathered trust level of a specific device has significantly changed, such as more than 10% of the previous trust level, then the device classification phase is initiated**.** The trust building and updating process is demonstrated in Fig. 4.

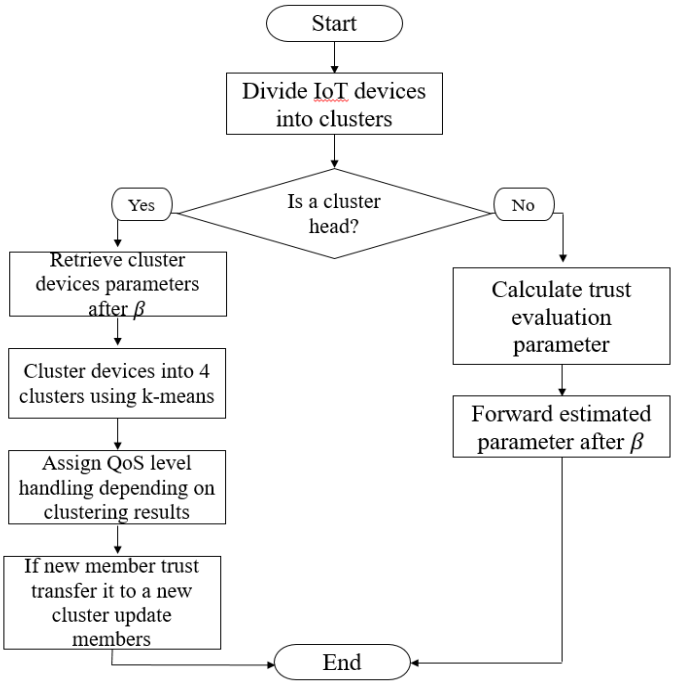

Fig. 4. Trust building and updating process.

3.6. QoS handling and guaranteeing.

When a QoS transaction is required, nodes retrieve the trust level of the destination node from the cluster head and send the data accordingly. Higher QoS level can also guarantee a lower level of QoS. Specially where devices are clustered in a higher value of trust. Data can be sent using a lower level of QoS defined in the other clusters. As shown in Fig. 5, when data is required to be sent with a QoS requirement, the source node asks CH to obtain the trust level of the destination. If the destination is located in a cluster with equal or higher QoS parameters, data can be sent with the required QoS parameters. Otherwise, the source can send the data with the QoS parameters of the retrieved cluster parameters, which is lower than the required QoS. Highest level of QoS can handle high traffic which needs a high level of QoS parameters like throughput or delay-sensitive traffic.

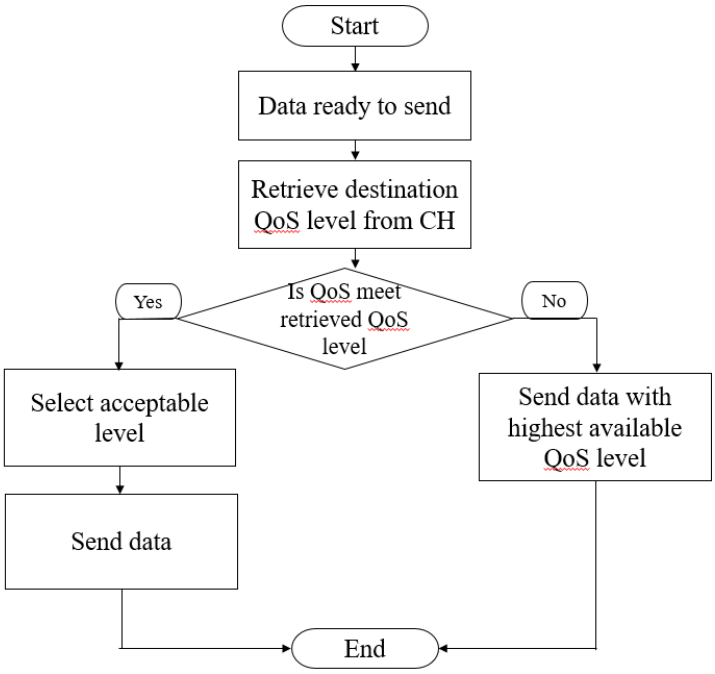

Fig. 5. QoS parameter handling.

3.7. Simulation parameter

As shown in Table 1, channel type used is a wireless channel, which connects all wireless nodes in the simulation scenario for data exchange [28]. In this scenario, the Radio-propagation model used is a two-ray-ground for long-distance communication [29]. The network interface type used is the wireless physical layer, which deals with four essential 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. Practically, this layer ensures adequate reception of the bit sent on the other side of the network [30]. 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 [31]. The MAC type is 802.11 NS-2 with its IEEE 802.11 support, which is extensively used for simulation of wireless communication in the research environment [32].

The topographical area was chosen to cover all units in clinics, big and small hospitals. The Routing protocol used is Ad Hoc On-Demand Distance Vector (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 [33]. The data flow used is a constant bit rate since this scenario needs to receive data at a constant bit rate like video data transfer to and from a digital video camera [34]. The packet size applied is 1000 bytes to enable the transfer of video data with high quality. The data bit rate of 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. Consequently, another factor that control the amount of data exchanged between the nodes [35]. This study considered a majority of health care systems ranging from small to large hospitals. Therefore, the scenario used in this simulation includes 50, 100, 150, and 200 nodes to cover the vast majority of healthcare centre units. Also, the effect of the number of nodes increase on energy consumption was investigated. The simulation time was selected to meet the expected amount of consumed energy and the initial energy [36]. The management of the network topology was widely ensured as a mechanism to enhance WSN lifespan [37]. The simulation time was selected to meet the expected amount of consumed energy and the initial energy.

The data bit rate chosen is 1 Mbps to meet the requirements of camera traffic. The main parameter considered for the trust model efficiency is the number of nodes. The simulation time was selected to meet the expected amount of consumed energy and the initial energy. Furthermore, most of these parameters are justified in [14].

Table 1. Simulation parameters.

PARAMETER	VALUE
Channel type	Wireless Channel
Radio-propagation model	Two Ray Ground
Network Interface Type	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
Number of IoT nodes	50,100,150,200
Simulation Time	50 seconds
Data Flow	CBR
Packet Size	1000 byte
Data Bit rate	1 mbps
Initial Energy	1000 Joule
RX Power	0.001
TX Power	0.001
Sleep Power	0.0001
Transition Power	0.0002
Idle Power	0.0001

4. Simulation and energy calculation

In the beginning, a brief description of the network simulator used was presented. Then, the performance evaluation metrics were defined to measure the performance of the recently proposed model and the proposed mechanism. Issariyakul and Hossain [38] have applied Network Simulator (NS2), where NS2 is an open-source software being used by the majority of Mobile Ad Hoc Network (MANET) community. Hence, estimating how events might occur in the real world there are many discrete event simulators available for MANET community. However, the most widely used software is reported to be NS2 [39].

The version of NS2-35 was used in the current study. In this paper, energy is the primary concern. Therefore, the main evaluation metrics include the average consumed energy, the average remaining energy, and the lowest remaining energy of the network node. NS2 simulator provides an energy model for simulating IoT and WSN devices. The energy model is a node attribute that represents the level of energy in a mobile node. class energy model determines the basic energy model in NS-2.35 with the following attributes tx power is transmitting power in watts, rx power is receiving power in watts, and initial energy is starting energy in joules. sleep power is consumed energy in sleep status and idle power is defined as consumed energy in the idle state where there are no activities. An update has been implemented on the energy model in NS2 to add a power sensing that indicates the amount of energy consumed during traffic monitoring.

4.1. Average consuming energy

This evaluation metrics mainly calculate the average value of the energy consumed at each IoT device. The consumed energy primarily depends on the required communication overhead in terms of sending, receiving, and sensing activities of each node. The consumed energy of each node can be calculated using the following Eq. (9).

$$En_{Cons} = En_{Send} + En_{Rec} + En_{idle} + En_{sleep} + En_{Mon} \quad (9)$$

Where En_{Cons} : the consumed energy, En_{Send} : energy consumed in sending data, En_{Rec} : energy consumed in receiving data, En_{idle} : energy consumed when the device is in idle state where no action is performed. En_{sleep} : energy consumed when the node is in the sleep state. En_{Mon} : the energy consumed when the node is monitoring or sensing data to other nodes. If a network contains *N* nodes, then the average consumed energy can be calculated using the following Eq. (10).

$$En_{Cons_{Avg}} = {\sum_{i=1}^{n} En_{Cons_i}}/{n} \quad (10)$$

where En_{Cons_i} is the consumed energy of the node *i*.

4.2. Average remaining energy

The average remaining energy indicates the average value of energy remained in the network nodes. It is mainly a real indication of the expected network lifetime.

The remaining energy can be calculated by subtracting the consumed energy from the initial energy, as shown in the following Eq. (11).

$$En_{Rem} = En_{Init} - En_{Cons} \quad (11)$$

where En_{Init} is the initial energy of the node, En_{Cons} is the consumed energy of the node. If a network contains *N* nodes, then the average consumed energy can be calculated using the following Eq. (12).

$$En_{Rem_{Avg}} = {\sum_{i=1}^{n} En_{Rem_i}}/{n} \quad (12)$$

4.3. Evaluation of QoS-energy aware trust module

In this section, the performance of the proposed QoS-Energy Aware Trust Model for IoT Devices (EA-IoT) is evaluated. A simulation topology was built to measure the evaluation the energy consumption, energy reaming, and minimum energy node remaining of the proposed mechanism against the recently proposed mechanism. The performance of the proposed mechanism was compared with the Sklavos et al. [40] which is discusses the Security & Trusted Devices in the Context of Internet of Things (STD-IoT). The second mechanism for evaluating performance is a trust management system design for the Internet of Things, which mainly considers context-aware and multi-service approach (Context-IoT) [20]. To assess the performance of the trust model, four different network topologies are designed to reflect the healthcare IoT device scenario. In this case, IoT devices are set to monitor the health parameters such as haemoglobin, pulse blood pressure, blood sugar, and surveillance cameras.

The scenario includes four different rooms with each location comprising 50 IoT devices [41]. In the simulation scenario, a single room is increased at each simulation cycle, so that the number of nodes is varied from 50 to 200 nodes with each room comprising a single CH. The simulation topology is shown in Fig. 6 for simplicity and simulation considering members located in four clusters and the QoS include four groups of services. However, it may vary based on the implementation scenario and clustering algorithm for QoS.

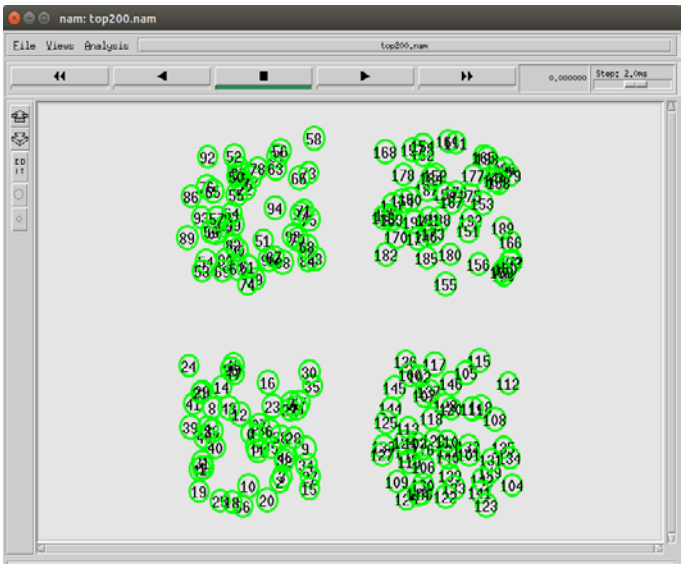

Fig. 6. The simulation scenario for 200 nodes.

5. Result

In this study, we proposed QoS Energy Aware-IoT (EA-IoT) model by considering QoS trust parameters, which are CT, DT, PT, and ET. K-mean algorithm was utilized to examine the energy consumption, energy reaming, and minimum energy node remaining for the proposed model, and the two previous model Context-IoT

and STD-IoT in the same simulation environment as shown in Table 1. However, the result showed in Table 2. the consumed energy for EA-IoT model considerably reduces when compared with previous studies Context-IoT and STD-IoT models.

Table 2. The average of energy consumed for Context-IoT, STD-IoT and EA-IoT models.

Model	50 nodes	100 nodes	150 nodes	200 nodes
Context-IoT	497	471.41	467	421.76
STD-IoT	491.9	502.11	498.1	434.48
EA-IoT	7.51	4.41	5.78	5.95

As a result of increasing the value of consumed energy for both previous studies Context-IoT and STD-IoT models, the value of the remaining energy is considerably decreased when compared with EA-IoT model as demonstrated Table 3.

Table 3. The average of remaining energy for Context-IoT, STD-IoT and EA-IoT models.

Model	50 nodes	100 nodes	150 nodes	200 nodes
Context-IoT	502	528.59	533	578.24
STD-IoT	508	497.88	501.89	565
EA-IoT	992.48	995.58	994.21	994

The minimum energy node results show that at least there is an exhausted node using both Context-IoT and STD-IoT models, where the minimum remaining energy of that node is equal to zero. However, EA-IoT model maintains a much higher level of energy with the minimum energy node as shown in Table 4.

Table 4. The minimum node energy for context-IoT, STD-IoT and EA-IoT trust models.

Model	50 nodes	100 nodes	150 nodes	200 nodes
Context-IoT	0	0	0	0
STD-IoT	0	0	0	0
EA-IoT	990	984.58	979.21	973

5.1. Investigating the effects of the number of cluster members

To further investigate the performance of the EA-IoT model against context-IoT and STD-IoT approaches. Experiments with different cluster members have been implemented. Five different simulation scenarios have been employed; the number of nodes was 10, 20, 30, 40, and 50. Simulation experiments demonstrate that EA-IoT model is slightly affected when the number of cluster members increased, as shown in Table 5. However, the consumed energy of STD-IoT is increased significantly when the number of nodes in a single cluster is increased. It almost remains constant when the number reaches 40 nodes in a single cluster.

Furthermore, the Context-IoT finding did not show by the number of cluster members. Therefore, the consumed energy remains almost constant with different number of cluster member.

Table 5. The average of energy consumed for context-IoT, STD-IoT and EA-IoT trust models using different number of cluster members.

Model	10 nodes	20 nodes	30 nodes	40 nodes	50 nodes
Context-IoT	502.13	526.99	532.61	488	497
STD-IoT	291	393.33	477.28	515.05	491.9
EA-IoT	3.14	6.5	7.12	6.16	7.51

The level of remaining energy reflects the same results shown in the consumed energy, as shown in Table 6. The remaining energy for EA-IoT model presents the highest values of remaining energy, where the remaining energy consumed for context-IoT model remains almost constant while cluster members number is increased. However, STD-IoT approach sharply decreases the remaining energy.

Table 6. The average of remaining energy for context-IoT, STD-IoT and EA-IoT trust models using different number of cluster members.

Model	10 nodes	20 nodes	30 nodes	40 nodes	50 nodes
Context-IoT	497.87	473.01	467.38	511.01	502
STD-IoT	709	606.67	522.72	484.94	508
EA-IoT	996.8	993.5	992.87	993.8	992.48

Table 7. presents the minimum remaining energy node levels. The results show that EA-IoT maintains the energy of the nodes in the cluster while Increasing the number of clusters. However, the minimum level of remaining energy at cluster nodes for STD-IoT model decreased sharply, and this node becomes entirely exhausted when the number of cluster members is greater than or equal to 40. This degrades the network performance and decreases the network's lifetime.

Furthermore, Context-IoT minimum remaining node is completely exhausted at all results despite the variance in the cluster 'member's number. Therefore, that it is not affected by the number of nodes in a single cluster. STD –IoT achieves better results than the Context-IoT model when the number of cluster members becomes smaller. However, when the members are increased, both STD-IoT and Context-IoT perform the same.

Table 7. The minimum node energy for context-IoT, STD-IoT and EA-IoT trust models using different number of cluster members.

Model	10 nodes	20 nodes	30 nodes	40 nodes	50 nodes
Context-IoT	0	0	0	0	0
STD-IoT	468.65	264.16	116.35	0	0
EA-IoT	994.95	992.4	991.8	992.3	990

6. Discussion

The finding of this study is considerably reducing the energy consumption comparing with the previous research for the trust model, as shown in Tables 2 and 3 The energy consumption, energy remaining, and minimum remaining node for the EA-IoT model are better than both Context-IoT and STD-IoT. The possible explanation for this difference could be that the mechanism for EA-IoT to calculating the trust and updating it to other nodes in a cluster reduces the number of communication messages used to build and update trust between nodes in

clusters. However, the context-IoT trust manager builds the trust model by fetching the trustworthiness of each node in the network after each task completion. Therefore, before any data communication step in the network, a query is sent to the trust manager asking to obtain the trust of the destination. Furthermore, the number of trust messages mainly depends on the number of data communication sessions in the network.

Moreover, STD-IoT sends a higher number of communication packets to build and maintain the trust model. The number of packets also depends on the number of nodes in the cluster as the gateway monitors the IoT devices. The trust is computed based on it, and the value is then sent to the IoT devices as a recommendation. Another possible explanation could be that the EA-IoT mechanism was calculating the final trust for each cluster member. As a result, the cluster head maintains these records when the trust value of the cluster member exceeds the threshold then the model will be updating.

The finding of this study is revealed that the members of each cluster are slightly effective on EA-IoT, a significant effect on STD-IoT, and not affected on Context-IoT, as shown in Tables 5, 6, and 7. In this scenario, the possible explanation for this outcome could be that the difference between the number of messages being sent. To compare, EA-IoT model sends a lower number of messages than STD-IoT model. The trust level in our proposed model remains at a specific level for a longer time of period without sending any new trust update messages to other nodes in that node clusters. However, the Context-IoT which mainly depends on the number of times that nodes send data communication that is not affected by the number of cluster members. Therefore, the consumed energy remains almost constant with the different number of a cluster member.

7. Conclusion and recommendation

The Internet of Things (IoT) has drawn significant research attention. IoT is considered as a part of the Internet of the future and will comprise billions of intelligent communications things. Different types of trust models were proposed to handle security and quality of services. However, these models do not consider energy in building the trust model or in updating the trust values. In this paper, an EA-IoT trust model is proposed where energy is regarded as a fundamental parameter in building and updating the trust model throughout the network lifetime. The required number of packets for trust update was considerably decreased. The proposed model is compared with two recent models, Context-IoT and STD-IoT models. Results showed that the EA-IoT model reduces the consumed amount of energy up to 98 % of both Context-IoT and STD-IoT models. Also, the amount of remaining energy has been significantly increased using EA-IoT by 50%, more than the Context-IoT model with 43%, than the STD-IoT model. In the Context-IoT and STD-IoT models.

Enhancements can be made in future research in the field of designing a QoS-trust model by considering the social trust factor for trust build and update. However, the proposed model did not cover security issues. Future research initiatives are encouraged to take into consideration a more comprehensive security approach taking into account such as block-chain technology.

Nomenclatures

C_T	Communication trust
D_T	Delay trust
$E2E$	End to End delay
En_{rec}	Energy consumed in receiving data
$En_{con\text{-}avr}$	Average of consuming energy
Enr_{cons}	Consumed energy
$Enr_{cons,\beta}$	Consuming energy rate at period of time β
En_{idel}	Energy consumed when the device is in idle state
En_{inti}	The initial energy of the node
En_{mon}	Energy consumed when the node is monitoring or sensing data
$En_{rem\text{-}avr}$	Average of remaining energy
$Enr_{rem,t0}$	Remaining energy at time t0
$Enr_{rem,\ t1}$	Remaining energy at time t1
En_{send}	Energy consumed in sending data
En_{sleep}	Energy consumed when the node is in the sleep state
E_T	Energy trust
F_β	Number of failed transmissions
K	Number of packets send by each node
P_T	Dependability trust
S_β	Number of successful transmissions
T_X	Transmission data.

Greek Symbols

β	Period of time

Abbreviations

AODV	Ad Hoc On-Demand Distance Vector
CH	Cluster Head
Context-IoT	Context-aware and multi-service trust management system
CPS	Cyber-Physical Systems
EA-IoT	Quality of Service Energy Aware Trust Model
IoT	Internet of Things
MANET	Mobile Ad Hoc Network
NS2	Network Simulator
QoS	Quality of Service
RFID	Radio Frequency Identification
STD-IoT	Security & Trusted Devices
TAEC	Trustworthy Agent Execution Chip
TRM-IoT	Trust Management Model
U2IoT	Unit and Ubiquitous
WSN	Wireless Sensor Network

References

1. Gubbi, J.; Buyya, R.; Marusic, S.; and Palaniswami, M. (2013). Internet of Things (IoT) A vision architectural elements and future directions. *Future generation computer systems*, 29(7), 1645-1660.

2. Alhasan, A.; Audah, L.; Alhadithi, O.S.; and Alwan, M.H. (2019). Quality of service mechanisms in internet of things: A comprehensive survey. *Journal of Advanced Research in Dynamical and Control Systems*, 11(2), 858–875.
3. Laplante, P.; and Applebaum, S. (2019). NIST's 18 Internet of things trust concerns. *Computer*, 52(6), 73-76.
4. Duan, J.; Gao, D.; Yang, D.; Foh, C.H.; and Chen, H.H. (2014). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet of Things Journal*, 1(1), 58-69.
5. Govinda, K.; and Saravanaguru, R.A.K. (2016). Review on IoT technologies. *International Journal of Applied Engineering Research*, 11(4), 2848-2853.
6. Khanouche, M.E.; Amirat, Y.; Chibani, A.; Kerkar, M.; and Yachir, A. (2016). Energy-centered and QoS-aware services selection for Internet of Things. *IEEE Transactions on Automation Science and Engineering*, 13(3), 1256-1269.
7. White, G.; Nallur, V.; and Clarke, S. (2017). Quality of service approaches in IoT: A systematic mapping. *Journal of Systems and Software*, 132(10), 186-203.
8. Yan, Z.; Zhang, P.; and Vasilakos, A.V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, 42(6), 120-134.
9. Safari, E.; and Babakhani, M. (2015). Web service and dynamic pricing competition. *International Journal of Industrial Engineering Computations*, 6(1), 99-116.
10. El-Sayed, H.; Mellouk, A.; George, L.; and Zeadally, S. (2008). Quality of service models for heterogeneous networks: Overview and challenges. *Annals of Telecommunications-Annales des Télécommunications*, 63(12), 639-668.
11. Awan, I.; Younas, M.; and Naveed, W. (2014). Modelling QoS in IoT applications. *Proceeding of the 17th International Conference on Network-Based Information Systems (NBIS)*. Salerno, Italy, 99-105.
12. Guo, J.; Chen, R.; and Tsai, J.J. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications*, 97(1), 1-14.
13. Al-Shammari, B.K.J.; Al-Aboody, N.; and Al-Raweshidy, H.S. (2017). IoT traffic management and integration in the QoS supported network. *IEEE Internet of Things Journal*, 5(1), 352-370.
14. Alhasan, A.; Audah, L.; Alabbas, A. (2020) Energy overhead evaluation of security trust model for IoT application. *Journal of Theoretical and Applied Information Technology*, 98(1), 69-77.
15. Chen, D.; Chang, G.; Sun, D.; Li, J.; Jia, J.; and Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, 8(4), 1207-1228.
16. Bao, F.; and Chen, I.R. (2012). Trust management for the internet of things and its application to service composition. *Proceeding of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*. San Francisco, CA, USA, 1-6.
17. Gessner, D.; Olivereau, A.; Segura, A.S.; and Serbanati, A. (2012). Trustworthy infrastructure services for a secure and privacy-respecting internet of things. *Proceeding of the IEEE 11th International Conference on Trust Security and Privacy in Computing and Communications*. Liverpool, UK, 998-1003.
18. Xu, X.; Bessis, N.; and Cao, J. (2013). An autonomic agent trust model for IoT

systems. *Procedia Computer Science*, 21, 107-113.

19. Ning, H.; Liu, H.; and Yang, L.T. (2013). Cyberentity security in the internet of things. *Computer*, 46(4), 46-53.
20. Saied, Y.B.; Olivereau, A.; Zeghlache, D.; and Laurent, M. (2013). Trust management system design for the internet of things: A context-aware and multi-service approach. *Computers & Security*, 39(11), 351-365.
21. Gu, L.; Wang, J.; and Sun, B. (2014). Trust management mechanism for internet of things. *China Communications*, 11(2), 148-156.
22. Chen, I.R.; Bao, F.; and Guo, J. (2015). Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing*, 13(6), 684-696.
23. Chen, I.R.; Guo, J.; and Bao, F. (2014). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing*, 9(3), 482-495.
24. Asiri, S.; and Miri, A. (2016). An IoT trust and reputation model based on recommender systems. *Proceeding of the 14th Annual Conference on Privacy, Security and Trust (PST)*. Auckland, New Zealand, 561-568.
25. Natkaniec, M.; Kosek-Szott, K.; Szott, S.; and Bianchi, G. (2012). A survey of medium access mechanisms for providing QoS in ad-hoc networks. *IEEE Communications Surveys and Tutorials*, 15(2), 592-620.
26. Yin, G.; Shi, D.; Wang, H.; and Guo, M. (2009). RepCom: Towards reputation composition over peer-to-peer communities. *Proceeding of the International Conference on Computational Science and Engineering (CSE)*. Vancouver BC, Canada, 765-771.
27. Shao, N.; Zhou, Z.; and Sun, Z. (2015). A lightweight and dependable trust model for clustered wireless sensor networks. *Proceeding of the International Conference on Cloud Computing and Security (ICCCS)*. Nanjing, China, 157-168.
28. Nayyar, A.; and Singh, R. (2015). A comprehensive review of simulation tools for wireless sensor networks (WSNs). *Journal of Wireless Networking and Communications*, 5(1), 19-47.
29. Eltahir, I.K. (2007). The impact of different radio propagation models for mobile ad hoc networks (MANET) in urban area environment. *Proceeding of the second International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless)*. Sydney, NSW, Australia, 30-30.
30. Radhakrishnan, R.; Edmonson, W.W.; Afghah, F.; Rodriguez-Osorio, R.M.; Pinto, F.; and Burleigh, S.C. (2016). Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view. *IEEE Communications Surveys and Tutorials*, 18(4), 2442-2473.
31. Puri, S.; Kaur, K.; and Kumar, N. (2014). A review of antennas for wireless communication devices. *International Journal of Electronics and Electrical Engineering*, 2(3), 199-201.
32. Malik, A.; Qadir, J.; Ahmad, B.; Yau, K.L.A.; and Ullah, U. (2015). QoS in IEEE 802.11-based wireless networks: A contemporary review. *Journal of Network and Computer Applications*, 55(9), 24-46.
33. Kim, J.M.; and Jang, J.W. (2006). AODV based energy efficient routing protocol for maximum lifetime in MANET. *Proceeding of the Advanced Int'l*

Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06). Guadelope, French, 77-77.

34. Kotian, P.J.; Vaishnavi, P.; and Begum, S. (2017). Review on data traffic in real time for MANETS. *International Research Journal of Engineering and Technology*. 4(11), 1632-1635.
35. Sharma, V.; You, I.; Andersson, K.; Palmieri, F.; Rehmani, M.H.; and Lim, J. (2020). Security, privacy and trust for smart mobile-internet of things (M-IoT): A survey. *arXiv:1903.05362*. 13(3), 1-45.
36. D'Angelo, G.; Ferretti, S.; and Ghini, V. (2017). Multi-level simulation of internet of things on smart territories. *Simulation Modelling Practice and Theory*, 73(40), 3-21.
37. Aparicio, J.; Echevarria, J.J.; and Legarda, J. (2017). A software defined networking approach to improve the energy efficiency of mobile wireless sensor networks. *KSII Transactions on Internet and Information Systems*, 11(6), 2848-2869.
38. Issariyakul, T.; and Hossain, E. (2012). *Introduction to network simulator 2 (NS2)*. Boston: Springer.
39. Singh, N.; Dua, R.L.; and Mathur, V. (2012). Network simulator ns2-2.35. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(5), 224-228.
40. Sklavos, N.; Zaharakis, I.D.; Kameas, A.; and Kalapodi, A. (2017). Security and trusted devices in the context of internet of things (IoT). *Proceeding of the Euromicro Conference on Digital System Design (DSD)*. Vienna, Austria, 502-509.
41. Rghioui, A.; L'aarje, A.; Elouaai, F.; and Bouhorma, M. (2014). The internet of things for healthcare monitoring: Security review and proposed solution. *Proceeding of the Third IEEE International Colloquium in Information Science and Technology (CIST)*. Tetouan, Morocco, 384-389.