Journal of Ubiquitous Systems & Pervasive Networks
Volume 15, No. 1 (2021) pp. 43-48

Internet of Things (IoT) based Network Integrated with Sensor Nodes for Intruder Detection and Low Energy Consumption

Gauri Kalnoor [a*], GowriShankar S [b]

[a] *Research Scholar, BMS college of Engineering, Karnataka, India*
[b] *Professor Computer science BMS college of Engineering, Karnataka, India*

Abstract

The applications in Internet of Things (IoT) for a large-scale Network which necessitates the storage resources and computing tasks, are gradually deployed in most of the wireless network environments. The computing model of traditional techniques when compared with features of cloud such as unlimited expansion, dynamic acquisition and pay-as-you-go are represented in different IoT architectures based on the conveniences of applications. Thus, one of the key challenges is to consider the service requirements when sensors are assigned to the tasks and the network performance is improved. In the presented work, the two-phase service system using Enhanced Bernoulli Vacation (EBV) scheduling algorithm and Intrusion Detection framework is proposed to minimize the energy consumed by the sensors while the service is provided. The performance variation of Virtual Machine (VM) and its achieved delay is considered, while first the tasks are divided into different tasks at different levels. The proposed work deals with a queuing system 'M/G/1' for Bernoulli Vacation scheduling model at one phase and intrusion detection technique at second phase. The sensing distance is also calculated with its density of network. The tasking scheduling algorithm is considered for execution cost and residual energy where the deadlines or threshold are proposed. The delay time, accuracy, detection rate and False Alarm Positive rate are evaluated during simulation time. Based on the work flows, experiments conducted are simulated for controlled tasks of IoT which demonstrates the algorithm achieving high success rate and that the network performs better when compared with the existing algorithms.

Keywords: *Security; Energy efficiency; Smart home automation; Internet of Things (IoT); safety; Sensor Network, Enhanced Bernoulli Vacation.*

1. Introduction

In the 21st century, the Internet of Things (IoT) is potentially the most supportive and overwhelming models of far-off correspondence. The growth of Science and Technology is growing rapidly with large scale data computing which cannot be differentiated from life sciences or scientific applications. The information's geometric growth [1] and its complexity of processing data makes the researchers in most of the disciplines, face various opportunities and challenges than ever. Different science applications such as prediction of disasters, Internet of Things (IoT) and gene sequencing are growing dependent on computing high performance and its distributed storage. Thus, the IoT based network depends on the reliable environment for computation and it has widely used in different types of fields. However, an IoT uses technology of sensing integrated within the network, which is considered to be an innovative mode of application. These types of network also include the communication technology and computing technology and are connected to massive devices to initiate real word interaction [2]. Thus, IoT realizes smart management of various objects and information through perception, the data is shared and exchanged with real time. Because of its own imitations in capacity, CPU, memory and battery of sensor nodes, the IoT applications have been facing the challenging issues and constrains while completing the tasks as they require the energy consumption at the end of the device and resources. Simultaneously, analysis, decision making and modelling design based on amount of data at the level of infrastructure of IoT are mostly difficult.

The IoT based smart home automation systems consists of actuators connected with various devices and the sensors that are positioned within the environment of home to supervise and control the operations of devices. Later, the local server connects to these integrated devices for data analysis and collection, through a wireless medium [3]. The main issue is, how to securely connect

* Corresponding author. Tel.: +919449975076
E-mail: Kalnoor.gauri@gmail.com

DOI: 10.5383/JUSPN.15.01.006

and transmit the analyzed data to the appropriate destination from the sensor node. Thus, there is a need for developing novel security techniques, and much research has been carried out based on which several mechanisms have been designed and proposed to overcome these challenging issues. The techniques may also include traditional encryption and security mechanisms designed for WSN's [4-6].

The networks with sensor nodes have limited constrained resources, such as memory, communication range, sensing distance, restricted battery power supply and limited capability of data processing [7-9]. The other challenging issues in these IoT based networks is how are these limited resources utilized efficiently for several applications in IoT. Thus, with this challenge, the algorithms for security should be designed and utilized to consume minimum energy and efficiently use the available resources within their networks. Moreover, many devices in IoT based smart home networks are connected from a very long distance, through the internet. Lastly, the third-most significant issue is how the coverage range can be increased such that the communication framework [10] can be combined with sensors and other backhaul networks. The IoT based smart home environment which is requires to be highly secured that can provide a balance between energy efficient security and security level algorithm implemented based on the mechanism of efficient key generation for encryption of data. Additionally, the network capability that supports communication at a long-distance coverage area among many numbers of IoT nodes is needed. In real life problems, queuing is one of the powerful tools which has been optimized and used as model to predict the waiting time and the queue length. This plays an important role in communication systems, supermarkets, restaurants, wireless sensor networks, hospitals, production lines etc. The basic idea of a queue is to provide a statistic and coordinated method based on the precedence of the service of the sensor. M/M/1/K is the queuing model used for scheduling and minimize energy.

Outline of the paper: The related work is discussed in section 2. In section 3, The proposed work is explained with a Model. The model of Intrusion detection system and queuing model is explained in section 4. The section 5 discusses about the results and performance analysis of the proposed work and concluded in section 6.

2. Related survey

The survey is performed based on the related field of research.

In [11], the author deals with queuing system 'M/G/1" with different phases of services and unreliable server consisting of period of failure and the delay period. The random set up period is estimated by the authors in their work, when the service channel fails for short time interval. Furthermore, the author has introduced the delay time with the breakdown period where the server remains idle until a threshold is built. The performance measures are experimented that determines the optimal threshold value. The author has further designed the model based on the arrival process of the server, and service as not been presented.

The authors in the article [12] has explained the mechanism for energy saving with a model of node operation in WSN. The work has been proposed using "threshold-controlled multiple policy of vacation" technique. The packet queues are directed to the network nodes when it becomes empty and a period of multiple vacation that is initiated during the receiving or transmitting of sensor node data packet, is blocked. According to the author, a fixed constant period is considered for successive vacations until 'N' number of packets are predetermined and accumulated. These accumulated packets in the queue are detected. The article also specifies that, at the vacation's completion epoch, the processes get restarted normally. The formulae for compact-form are the distribution of processing and idle period respectively. Thus, the numerical examples are presented and derived in the work by the authors.

The author in the article [13] considers the major issues in IoT and highlights on the energy consumption model using data encryption technique. The sensor networks provide the benefits over traditional methods for applications like smart homes, environmental monitoring, healthcare and home land security. A new approach called "Triangle Based Security Algorithm (TBSA)" is proposed by the author for enhancing security in the network. This algorithm is based on the mechanism of generation of key. The author has also discussed about integration of Low power Wi-Fi in WSNs through internet to obtain secure data transmission among several sensor nodes in the IoT based smart home environment. But the author has not been considering the accuracy of detection of intruders to increase the performance of the network.

The performance of network based on Queueing systems in which cost analysis is one of the important factors is discussed by author in [14]. A Genetic Algorithm (GA) is employed to construct the cost model and then optimum values are determined based on the parameters. It's intelligent procedure of searching is utilized to find the fittest and also best design solutions. The author mentions that using other optimization techniques, it is difficult to find the best solutions for design.

The articles in [15-17] represents M/G/1 queuing model in which the authors have considered different mathematical models to represent energy efficient networks. In the last decades, the systems based on vacation queues were investigated exclusively because of their applications in different fields, for instance, communication networks, computer system, etc. The past work of research can be classified into categories of server vacation and working vacations as discussed by the authors in [18][19].

3. Proposed Model Description

From the analysis performed, it was seen that the current calculations looked more force than the proposed MBVS, in light of the fact that they require more complex methods and overhead to make sure about the first data. The MBVS calculation has been exceptionally created for all applications including the transmission of data between remote sensor hubs. As sensor hubs in WSNs have restricted asset issues, for example, memory, limited power and information processing power, the MBVS technique is utilized as a potential answer to accomplish energy proficient security. The algorithm below shows the Enhanced Bernoulli Vacation Scheduling for minimizing the energy consumption.

3.1. Enhanced Bernoulli Vacation (EBV) Scheduling Algorithm:

1.Initialization: Obtain threshold T.
2 set N = 0
3 wait for Max-Age
4 if sensed value changed then
5 send response message to proxy
6 goto step 2
7 else
8 generate random number t from a Bernoulli distribution with mean of 1
N :
9 if t < T then
10 send response message to proxy
11 goto step 2
12 else
13 N = N + 1

3.2. Energy Consumption Estimation:

In the insightful arrangement of the proposed framework, an energy model of each sensor hub, which the organization utilizes in each activity, is incorporated to decide the framework's exhibition. In the model, the condition used to show every hub's energy utilization is:

$E_{Tx} = E_{elec}$ + pEampR2comm

ERx = Eelec

where ETx and ERx are the communicated and gotten forces of a sensor hub for every piece, individually, Eelec the energy of an electron and Eamp the speaker energy. This model is utilized in the proposed framework on account of its straightforwardness. During the inactive state, it is assumed that the model doesn't burn through any effort. Albeit, this supposition that is false, being inactive the information accepting expense is excessively short contrasted with the aggregate sum of cost the organization will be dynamic. Consequently, the energy utilization in the inactive state is immaterial.

A) M/M/1/K Queuing Model (Fluid Queue Model)

The queuing model M/M/1/K [20] is the simple trivial queuing system where the nodes arrive with the rate λ, most commonly based on the Poisson process. The model describes the intermediate arrival time as independent, and random variables distributed exponentially using parameter λ. The sensors are active and the service times are considered as independent and exponentially allocated using parameterμ. Thus, all the random variables involved are assumed to be self-governing to each other as shown in the figure 4:

$$Let\ \rho = \frac{\lambda}{\mu} < 1, then\ C_N = \left(\frac{\lambda}{\mu}\right)^N = \rho^N\ for\ N = 1, 2, 3, \dots\dots$$

$$Therefore\ P_N = C_N P_0\ Now, the\ normalizing\ condition\ is \sum_{N=0}^{\infty} P_N = 1 \quad \text{----------(1)}$$

3.3. Intrusion Detection System Model

For many number N and a small probability p, the binomial representation is represented by the Poisson procedure. The mean value estimated by using equivalent Poisson process is,

$$N_p = \frac{N\pi R_{SENS}^2}{S_{area}} \text{----------(2)}$$

The probability of the sensing model to detect an intruder by 'k' number of sensor nodes is followed by the Poisson distribution and is specified by the trailing formulation:

$$P(n = k) = \frac{(S\lambda)^2}{k!} e^{-(s\lambda)} \text{----------(3)}$$

where S is represented as area that is brushed by an intruder followed by course I, assuming that the intruder makes a move in a haphazard fashion starting from any random point, as shown in the figure 1:

$$s = 2R_{SENS} l + \pi R_{SENS}^2 \text{----------(4)}$$

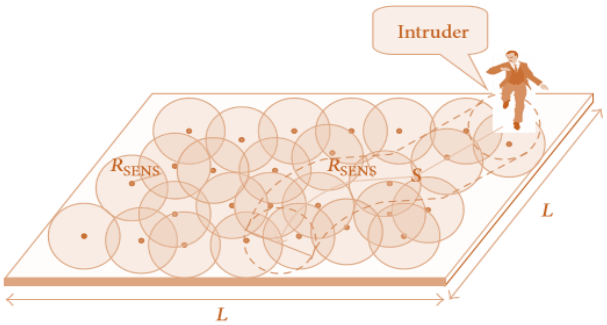

Figure 1: A simple scenario of intrusion. Here, the intruder starts at a random point and makes a move within the surface area S with a trajectory l. The moves made are in random fashion in WSN.

The probability calculated earlier is further represented by the succeeding equation:

$$P(n = k) = \frac{\left((2R_{SENS} l + \pi R_{SENS}^2)\lambda\right)^2}{k!} e^{-(2R_{SENS} l + \pi R_{SENS}^2)\lambda} \text{-(5)}$$

Thus, the distance of an intruder l is derived using the length of an arc of parametric curve as expressed with the formula shown below:

$$l = \int_a^b \sqrt{(f'(x))^2 + (g'(x))^2}\, dx \quad \text{----------(6)}$$

Further the numerical analysis is performed as discussed below [21]:

(1) The network is empty with probability

$$P_0 = P_{0,0} + P_{0,2} = \frac{(\lambda+\theta)\theta(1-\rho)(1-\bar{p}\widetilde{G_v}(\theta))}{(\theta(\lambda+\theta)+\lambda^2(1-\gamma))\left(1-\bar{p}\widetilde{G_v}(\theta)\right)-\lambda(1-\gamma)(p\theta+p\lambda))\widetilde{G_v}(\theta)} \quad (7)$$

(2) The sensor is idle with probability

$$P_{0,2} = \frac{\theta^2(1-\rho)(1-\bar{p}\widetilde{G_v}(\theta))}{(\theta(\lambda+\theta)+\lambda^2(1-\gamma))\left(1-\bar{p}\widetilde{G_v}(\theta)\right)-\lambda(1-\gamma)(p\theta+p\lambda))\widetilde{G_v}(\theta)} \quad (8)$$

(3) The sensor is in a working vacation with probability

$$P_{0,0} + P_0(1) = \frac{\lambda(1-\rho)\left[\theta\left(1-\bar{p}\widetilde{G_v}(\theta)\right)+\lambda(1-\gamma)\left(1-\widetilde{G_v}(\theta)\right)\right]}{(\theta(\lambda+\theta)+\lambda^2(1-\gamma))\left(1-\bar{p}\widetilde{G_v}(\theta)\right)-\lambda(1-\gamma)(p\theta+p\lambda))\widetilde{G_v}(\theta)} \quad (9)$$

(4) The sensor is in the busy period with probability

$$P_{0,0} + P_0(1) = \frac{p\left[\theta(\lambda+\theta)(1-\bar{p}\widetilde{G_v}(\theta))+\lambda(1-\gamma)(\lambda\left(1-\widetilde{G_v}(\theta)\right)-\theta\widetilde{G_v}(\theta))\right]}{(\theta(\lambda+\theta)+\lambda^2(1-\gamma))\left(1-\bar{p}\widetilde{G_v}(\theta)\right)-\lambda(1-\gamma)(p\theta+p\lambda))\widetilde{G_v}(\theta)} \quad (10)$$

(5) The mean Queue Length is

$$E[L] = P'(1) = \lim_{z\to 1} \frac{P_{0,0}}{\lambda} \frac{D'(z)N''(z)-N'(z)D"(z)}{2D\prime(z))2} = \frac{N"}{2N\prime(1)} - \frac{D"(1)}{2D'(1)} \quad (11)$$

where,

$\alpha = B'(1)$,

$D'(1) = 1 - \rho\left(1 - \overline{p\widetilde{G_v}(\theta)}\right)$,

$D"(1) = 2(1-\rho)(1-\bar{p}\alpha) - \lambda^2\beta^{(2)}(1-\bar{p}\tilde{G}(\theta))$

$N'(1) = \frac{\left(\theta(\lambda+\theta)+\lambda^2(1-\gamma)\right)(1-\bar{p}\tilde{G}(\theta))+\lambda(\gamma-1)(\theta\rho+p\lambda)\tilde{G}_v(\theta))}{\theta}$

$N"(1) = 2(\lambda+\theta)\left[(1-\bar{p}\alpha)+\rho(1-\bar{p}\tilde{G}(\theta))\right] - 2\lambda(2-\gamma)\left[\rho\widetilde{G_v}(\theta) - \frac{\lambda}{\theta}(1-\widetilde{G_v}(\theta))\right] + \lambda(\gamma-1)\left[\lambda^2\beta^2\widetilde{G_v}(\theta) - \left(\frac{2\lambda^2}{\theta^2}+\frac{2\rho\lambda}{\theta}\right)\left(1-\widetilde{G_v}(\theta)\right) + 2\alpha(\rho+\frac{\lambda}{\theta})\right]$

4. Results and Discussion

In this section, the best results are tabulated and have considered 2 case studies which are compared and presented based on the results obtained in the past experiments for performance metrics. The first objective is to minimize the energy consumed by the sensors IoT based WSNs, a proper node deployment scheme has to be selected as the density of its nodes which determine the life-span of a network. Therefore, to extend the monitoring system's lifetime, this density must be scalable with the monitoring area. From the results, the mode of sensors during data transmission is tabulated and the density with sensing range is estimated for N number of nodes.

Technique/Method with Energy Consumption (Micro Joule/Byte)
1 Proposed EBV 0.20
2 RC 4 0.49
3 Blowfish 0.81
4 AES 1.20
5 DES 2.80

Case 1: Nodes are:

Name	: [1×50 double]
Density	: [1×50 double]
Sensing distance	: [50×50 double]
Distance Covered by Intruder	:16917.1383units

Results in = 50×3 table

Case 2: Nodes are:

Name	:	[1×50 double]
Density	:	[1×50 double]
Sensingdistance	:	[50×50 double]

Distance Covered by Intruder:33832.5272units
Results in = 50×3 table

The Probability of detecting the Intruder in this WSN:0.95073

Transmission delay:

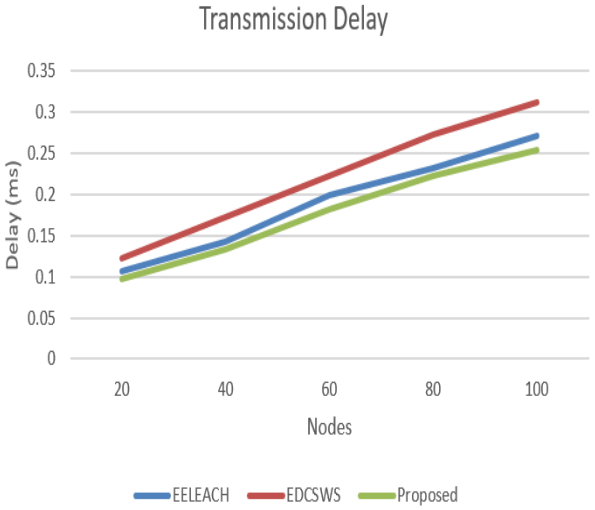

Figure 2: Number of nodes versus transmission delay

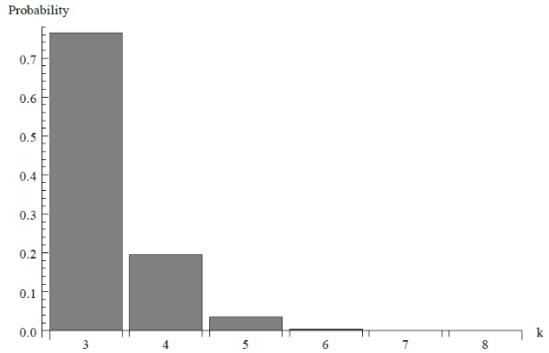

Figure 3: Number of packets of at the completion epoch of vacation period for $\lambda = 0.8$.

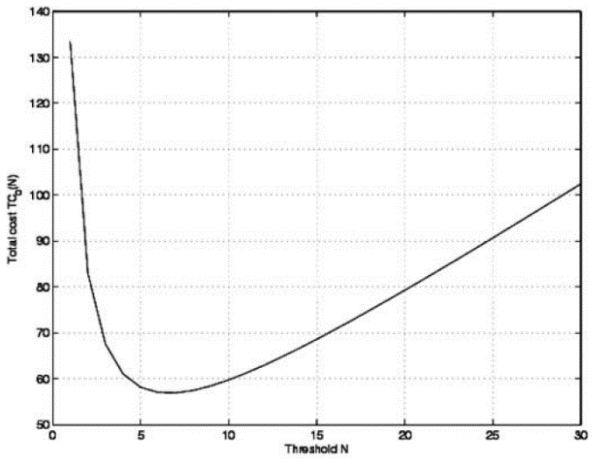

Figure 4: Total Cost with per unit time

Comparative analysis

The results obtained during simulations are compared with the existing methods of Intrusion Detection in IoT based systems. Table 1 represents the comparison of performance analyzed.

Table 1: Comparative Analysis

	Technique/Method	**Energy Consumption (Micro Joule/ Bytes)**
1	Proposed Enhanced Bernoulli Vacation (EBV)	0.17
2	TBSA	0.20
3	MD4	0.50
4	HMAC 1	1.10
5	SHA-1	0.75

The analysis of energy consumption is made and calculated for the proposed work. The performance evaluation metrics is shown in the figure 5 with minimum energy consumption for the proposed algorithm.

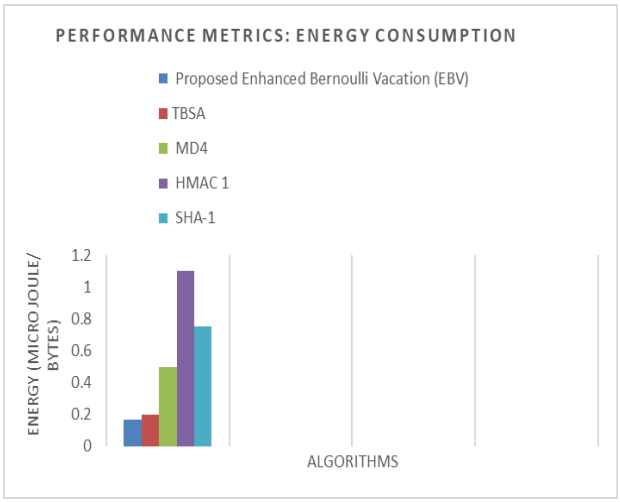

Figure 5: Energy Consumed for various algorithms

5. Conclusion

The work is analyzed based on the proposed model of Enhanced Bernoulli Vacation scheduling where the Single Sensor Delayed Vacation and Number of sensor nodes Service starting failures and two types of operation are compared. The sleep/wake rule is applied in the queuing system to reduce the energy consumed by the sensors. The sensor nodes integrated in IoT are resource constrained and also less secured. Thus, intrusion detection mechanism is applied by estimating the sensing distance of the sensors. The simulation is performed with evaluation metrics as energy consumption, sensing range, accuracy, density of nodes, vacation period time and delay. A vacation queuing models with sensor vacation depends on the batch sizes in this present work and the state of switching over is taken into consideration. The exploration on the current examination can be additionally stretched out by including the ideas of working breakdown, Bernoulli vacation. Application of this paper results are useful to healthcare system, communication networks, manufacturing process and transportation, production lines and mail systems.

References

[1]. W.L. Li, Y.N. Xia, M.C. Zhou, et al., Fluctuation-aware and predictive workflow scheduling in cost-effective infrastructure-as-a-service clouds. IEEE Access 6, 61488–61502 (2018).

[2]. G. Yao, Y.S. Ding, Y.C. Jin, et al., Endocrine-based coevolutionary multiswarm for multi-objective workflow scheduling in a cloud system. Soft. Comput. 21, 4309–4322 (2017).

[3]. F. R. B. Cruz1 and T. van Woensel, Finite Queueing Modeling and Optimization: A Selected Review, Journal of Applied Mathematics, 2014, 1–10.

[4]. K.Thiyagarajan and Dr.K.Mohan Kumar, Optimized Server Utilization In Multi Speciality Hospital By Using The Queuing Model Through IoT, International Journal of Scientific and Technology, 8(10)(2019), 1–10.

[5]. Vijaya Laxmi, P, and V Suchitra. Finite Buffer GI/M(n)/1 Queue with Bernoulli-Schedule Vacation Interruption under N-Policy, International Scholarly Research Notices, 2014.

[6]. Madhu Jain and Anamika Jain, Working vacations queueing model with multiple types of server breakdowns, Applied Mathematical Modelling, 34(1)(2010), 1–13.

[7]. Q.W. Wu, F. Ishikawa, Q.S. Zhu, et al., Deadline-constrained cost optimization approaches for workflow scheduling in clouds. IEEE Transactions on Parallel and Distributed Systems 28(12), 3401–3412 (2017).

[8]. Pavai madheswari. S, Krishnakumar. B and Suganthi. P, Analysis of M/G/1 retrial queue with second optional service and customer balking under two types of Bernoulli vacation schedules, Rario, Operations Research, 53(2)(2019), 415–443.

[9]. Kempa, W.; Marjasz, R. Departure counting process in a wireless network node with sleep mode modelled via repeated vacations. In Proceedings of the 23rd International Conference on Information and Software Technologies (ICIST), Druskininkai, Lithuania, 12–14 October 2017; pp. 395–407.

[10]. Vijaya Laxmi, P., and V. Suchitra. "Finite Buffer Queue with Bernoulli-Schedule Vacation Interruption Under-Policy." International scholarly research notices 2014 (2014).

[11]. Kempa, Wojciech M. "Analytical Model of a Wireless Sensor Network (WSN) Node Operation with a ModifiedThreshold-Type Energy SavingMechanism." Sensors 19.14 (2019): 3114.

[12]. J. Sahni, P. Vidyarthi, A cost-effective deadline-constrained dynamic scheduling algorithm for scientific workflows in a cloud environment. IEEE Transactions on Cloud Computing 6(1), 2–18 (2018).

[13]. V. Arabnejad, K. Bubendorfer, B. Ng, Budget and deadline aware e-science workflow scheduling in clouds. IEEE Transactions on Parallel and Distributed Systems 30(1), 29–44 (2019).

[14]. J. Meena, M. Kumar, M. Vardham, Cost effective genetic algorithm for workflow scheduling in cloud under deadline constraint. IEEE Access 4, 5065–5082 (2016).

[15]. Z. Shelby. RFC 7252: The constrained application protocol. https://tools.ietf.org/html/rfc7252, 2014.

[16]. H.-W. Kang and S.-J. Koh. Enhanced group communication in constrained application protocol-based internet-of-things networks. Int. J. of Distributed Sensor Networks, 14(4):1–14, 2018.

[17]. J. Miˇsi´c and V. B. Miˇsi´c. Proxy cache maintenance using multicasting in CoAP IoT domains. IEEE Internet of Things Journal, 2018.

[18]. F. M. Kovatch. Scalable Web Technology for the Internet of Things. PhD thesis, ETH Z¨urich, Switzerland, 2015.

[19]. M. Kovatsch, M. Lanter, and Z. Shelby. Californium: Scalable cloud services for the internet of things with CoAP. In Internet of Things (IOT), 2014 International Conference on the, pages 1–6. IEEE, 2014.

[20]. A. Borshchev. The Big Book of Simulation Modeling. Multimethod Modeling with AnyLogic. Anylogic North America, Chicago, IL,2013.

[21]. Haque, M.E.; Hannan, M.A. Toward Optimum Topology Protocol in Health Monitoring. Perform. Internet Things 2019, 81–109.

[22]. Walid, B.; Challal, Y.; Bouabdallah, A.; Tarokh, V. A highly scalable key pre-distribution scheme for wireless sensor networks. IEEE Trans. Wirel. Commun. 2013, 12, 948–959.