Robust Modelling to Jointly Address Security Threats, Bandwidth Utilization, and Energy issues in IoT

Bhagyashree Ambore, Suresh L

Abstract*: *The advent of Internet-of-Things (IoT) revolutionizes the mechanism of connectivity of massive chains of machine offering better improvement in data communication and analytical services. Review of existing approaches towards IoT performance improvement shows that there are still larger scope of enhancing the present solution. The proposed system introduces a mechanism where 3 different problems has been jointly addressed viz. security issues, channel capacity issues, energy depletion issues. The proposed model uses analytical research methodology where energy problem is offered common focus and linked with other two problem using stochastic method, probability logic, decision-making approach, packet scheduling, etc. The simulation outcome of the study shows that proposed system offers better energy efficiency, better resistivity against threats, and effective optimization of the bandwidth in contrast to existing related mechanism towards IoT ecosystem.

Keywords* : *Internet-of-Things, Security, Bandwidth, Energy Resource

I. INTRODUCTION

The evolution of Internet-of-Things (IoT) has re-defined the process of massive connectivity of the communication and computing devices called as machines [1]. Basically, IoT involves combination of multiple disciplinary technologies that combine together to make the complete system functional [2]. At present, the mechanism of working principle in IoT involves various applications in the form of smart homes, consumer application, healthcare services, energy management, elder care, transportation, infrastructure application, home automation, agriculture, vehicular communication, manufacturing application, etc [3][4]. There are various issues and challenges associated with the IoT that has been discussed by many researchers [5] [6]. However, out of all problems, there are some set of problems that are immensely critical and need immediate solution. The primary potential problem in IoT is the security and privacy concerns [7]. There are various forms of threats whereas the existing solution is incapable of handling those threats effectively. Such threats are formed from higher scale of interconnected machines with the cloud system that has higher chances to get compromised. Another essential problem with IoT system is its inferior design over varied protocols with highly sophisticated configuration and moreover there is less availability of robust technologies connected to IoT connected with the complex business process. It is also found that maintenance of life cycle as well as management of it is quite a complex process as there is highly restricted assistance for this purpose. Apart from this there are no reported standard or optimal implementation protocols and exercises meant for developers of IoT. Because of this problem, the architectural design of the IoT is limited to either few numbers of nodes or involving homogenous nodes with similar forms of environmental information, which contradicts the theory of application and capability supported by IoT. As IoT involves resource constrained nodes connected with the gateway system in order to perform autonomous transmission of data, there is always a problem of effective bandwidth utilization. As bandwidth is fixed by the service provider for the IoT devices but that bandwidth will never be sufficient for proper operational activity if the incoming traffic is of highly dynamic form of consider high-dimensional data [8-9]. Hence, offering an effective bandwidth for the massively connected IoT nodes is really a challenging problem. Finally, the potential problem associated with an IoT application is the energy dissipation problem. The prime reason behind it is that majority of the IoT application makes use of sensors which uses fixed amount of energy to be allocated while performing communication task. It will mean that energy allocated for the IoT devices are directly proportional to amount of the energy that has to be allocated. Hence, handling of massive stream of traffic will lead to faster drainage of the energy of IoT nodes. Therefore, energy, bandwidth utilization, and security are the prominent problem that requires an immediate attention from the researchers. There is a strong connectivity between the energy and security as majority of the security approaches in IoT uses encryption-based approaches that are not only recursive in its operation but also consumes maximum resources while performing security operation. Hence, the prime purpose of the proposed system is to formulate a novel mechanism where all these three unsolved problems are addressed effectively. For this purpose, the proposed system offers solution by using an analytical-based modeling where proposed mechanism targets to optimize the overall performance of the IoT nodes using cost effective solution.

Revised Manuscript Received on December 30, 2019.

***** Correspondence Author

Bhagyashree Ambore*, Assistant Professor, Department of Computer Science and Engineering, CITech, Bangalore, India. Email: ambore.bhagyashree@gmail.com

Suresh L, Pricipal and Professor, Department of Computer Science and Engineering, CITech, Bangalore, India.

The organization of the proposed paper is as follows: Section 1.1 discusses about the existing literatures where different techniques are discussed for improving IoT based operation with respect to bandwidth, security, and energy problems followed by discussion of research problems in Section 1.2 and proposed solution in 1.3. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

A. The Background

At present, there have been various studies being carried out emphasizing over the performance improvement of cloud that is highlighted in our prior work [10]. The recent work carried out by Alsaryrah et al. [11] has used optimization scheme for controlling energy consumption of IoT nodes as well as upgrading the quality of service factors. Bhattarai and Wang [12] have discussed about significance of security over IoT system and presented an adversary model for highlighting the concerns associated with privacy. Bisadi et al. [13] have presented a discussion about energy management system and presented architecture towards solving it. Existing system has also reported usage of task scheduling for energy preservation where dynamic programming is used as seen in the work of Caruso et al. [14]. Harvesting kinetic energy is presented as a solution toward energy depletion problems in IoT reported by Ju et al. [15]. Mansilla [16] has presented a decision-making process for energy efficiency for office buildings. Adoption of energy harvesting scheme is shown to offer added advantage towards energy problems in IoT especially when resource constrained Rectenna is used. Shafique et al. [17] have presented experimental-based model for proving this concept. Roy et al. [18] have presented a discussion about communication protocol which is energy efficient and can run over a longer period of time over dynamic environment of communication. Zhai et al. [19] have presented a stochastic based modeling where a decision-based approach is presented for scheduling user that can further facilitate in effective allocation of power. Mozaffari et al. [20] have presented an energy-efficient protocol for unmanned vehicles in IoT application. Apart from energy efficiency and security, the existing work has also been emphasized over channel capacity. Ji et al. [21] have discussed the significance of visual IoT applications with respect to its applicability over smart city. The relationship between channel capacity and contents is discussed by Lee et al. [22] where the optimization of the bandwidth is discussed. Cao et al. [23] have highlighted the usage of embedding of virtual network using node ranking methodology for controlling the utilization of the resources. Hou et al. [24] have presented a planning of bandwidth and scheduling virtual machine for solving resource saturation problem. Kua et al. [25] has used queuing technique for controlling the channel capacity in order to offer seamless service relaying over IoT based application. Hou et al. [26] have used harvesting of energy for efficient resource utilization inIoT. Huang et al. [27] have targeted harvesting approach over devices in ioT that uses software defined network for better service relaying to balance energy consumption and quality of services. Existing literature has also claimed beneficial usage of machine learning approach for enhancing the consumption of energy in IoT as seen in work of Javed et al. [28]. Long et al. [29] have presented an energy-aware routing scheme for massive scale of deployment of IoT nodes. Discussion of fog-based energy management scheme was carried out by Moghaddam et al. [30] emphasizing over delay and bandwidth. The next section discusses about the open end problems associated with it.

B. The Research Problem

The significant research problems are as follows:

- Existing energy efficiency scheme mainly reported to use harvesting scheme without offering a proof of overhead in communication due to inclusion of harvesting module.
- Existing energy efficient schemes are found to addressed but without any joint consideration of its associated problems e.g. bandwidth security, etc.
- Cost effective security approach are found in lesser proportion in existing system which is also the reason of energy depletion in faster rate.
- Improvement of data communication in IoT demands better planning of data forwarding scheme which is seen less effectively investigated in existing system.

The statement of the problem after reviewing is "*Developing a cost effective framework for resisting the significant problems connected with the resource constrained IoT nodes in presence of dynamic topology is quite challenging task.*" The next section outlines solution to the above stated issues.

C. The Proposed Solution

The implementation of the proposed system is carried out using analytical research methodology where the main focus is towards achieving multiple factors that are essential for proper operation of IoT nodes. For IoT nodes to be perfectly working, it is necessary that they should be energy efficient as such nodes are required to capture and process higher streams of data and hence larger value of energy efficiency is always depleted. The second essential thing is that an IoT node will be required to offer an efficient bandwidth management as massive size of the streamed data is allocated to the communicating devices which requires a fair sharing of the allocated bandwidth capacity. Finally, the essential component will be to provide security as different forms of communicating devices are exposed to different levels of threats that are essential to be identified. The block diagram of the methodology adopted for the proposed system is as shown in Fig.1.

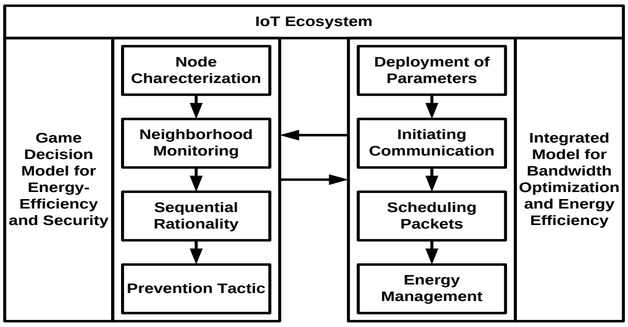

Fig.1. Block Diagram of Proposed System

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

According to the proposed system shown in Fig.1, it can be seen that it is classified into two essential methods where the first methods deals with the energy and security efficiency while the second method is associated with energy management and effective optimization of bandwidth. The first method uses game theory logic where a challenging adversary environment and its mitigation technique is constructed using sequential rationality concept. A prevention strategy has been developed that offers resistivity against any form of threats in distributed and large wireless network environment. The second model introduces the packet scheduling or provisioning practices along with energy management that offers more benefits towards cost effective and superior communication performance among the resource constrained IoT nodes. The proposed system.

II. SYSTSEM DESIGN IMPLEMENTATION

This part of study makes use of the analytical research methodology where the probability logic is used for the modeling purpose. It is to be noted that proposed system has targeted to offer the dual objectives which are associated with security and bandwidth optimization with a common target of energy efficiency to be achieved. This section discusses about the assumptions and dependencies, implementation strategy, as well as core design modules.

A. *Assumption & Dependencies*

The *primary assumption* of the proposed study is that all the sensory nodes are considered to be an integral part of the IoT ecosystem. This assumption will mean that all the sensor nodes are bound by execution of conventional communication standards in IoT connected with cloud services. The *secondary assumption* of the proposed system will mean that all the communicating devices involved in IoT ecosystem has allocation of specific amount of resources that cannot be scaled up individually. This assumption will let the proposed implementation to adhere in resource-constraint environment in order to roll out with practical solution. The *tertiary assumption* of the proposed system is that the network is exposed to various forms of threats and there is already a firewall system running underlying the IoT network; however, there is no predefined information about the types of threats and their level of severity. This assumption will offer better applicability of proposed system to offer security in absence of any apriori data of intrusion. The dependency of the proposed study is that it uses heterogeneous nodes formulated in the form of clusters to make group-wise communication with each other.

B. *Implementation Strategy*

The proposed system targets to achieve energy efficiency, bandwidth optimization, as well as security at same time and hence it has to be formulated in the form of holistic architectural-based approach. Therefore, the first implementation strategy is to apply divide and conquer policy while splitting the complete work in two levels of implementation viz. i) the first implementation level will be towards achieveing security and energy efficiency and ii) the second implementation level will be towards achieving bandwidth optimization and energy efficiency. The implementation strategy of the first level of work is about identifying the susceptible behaviour of the attacker which is quite challenging one. It is challenging because attacker node will have less information about the security protocol running and there are good chances of getting themselves identified by the security protocols being assumed to be executed by good nodes. Hence, attacker node will get more involved in data forwarding process in order to increase their trust level in such an extent that they achieve reliability. This scenario was important to be implemented as it will offer equal strength to attacker node to launch an attack while it also offer equal opportunity for regular node to identify the malicious intention of attack. Therefore, it is nearly challenging to identify the attacker. This problem is solved by implementing neighborhood monitoring concept where the dynamic trust factor is always under surveillance. By observing the dynamic trust factor, the proposed system finds for an event when the ambiguity factor of any node is found to be high. Using the concept of game theory, the proposed study develops a mechanism where on the basis of resource consumption pattern monitoring of the malicious activity is carried out. In this entire process, there is absolutely no usage of encryption which makes the proposed system unique and non-iterative and free from any possibility of encryption-based attacks. The next part of the implementation level is about bandwidth management and energy efficiency which uses analytical approach. The study develops a new mechanism of internal message construct where special focus is laid on the message priority in order to improve the faster communication process in case of critical applications. Adoption tree mechanism, the proposed system considers both static as well as random position of the IoT nodes where a better form of assessment environment is constructed. The proposed system also implements an exclusive packet provisioning mechanism that can perform the better communication process via IoT gateway nodes. Finally, a simplified energy modeling is carried out which ensures that only necessary amount of energy has to be allocated for communicating nodes in order to make communication. This energy is empirically calculated for the entire communicating node with an objective that efficient bandwidth management has to take place. This mechanism ensures traffic flow of essential data packets first followed by dynamic update of the active queue system on the basis of the current traffic condition. Therefore, a closer look into the proposed implementation strategy will exhibit that it implements a simplified and cost effective mechanism in IoT ecosystem where better form of communication can take place. The next section discusses about core modules of the study.

C. *Game Decision Model for Energy-Efficiency and Security*

This is the first part of the implementation of the proposed system where the idea is to perform optimal security system for all the wireless nodes and devices connected using IoT system. Fig.2 highlights the block diagram of the the proposed study which shows the significant usage of game theory. According to this concept, the proposed system doesn't consider any pre-defined trust value for any communicating nodes (be it relay node or direct destination node) and rather it performs computation of the trust factor of the communicating nodes. For this purpose, the proposed sysem formulates multiple strategic implementations. The first part of the implementation is about formulating the capturing process for the malicious nodes where the logic is to allocate some common and some distinct set of operation that can be performed by good node as well as harmful node. The justification behind this logic is to render the identification system quite challenging for offering precision in detection of motive of the nodes. The proposed system uses probability theory in order to model this logic where the occurances of the common set of operation are quite higher than that of distinct set of operation. This is also going to be the best test cases to assess the robustness of the proposed evaluation system. The proposed system offers a significant mechanism of intrusion detection system where the resource factor plays a significant role. The rationale behind consideration of the resource factor is that a malicious node is basically meant for launching malicious program within the transmission area; however, the major problem is that it cannot instantly launch malicious program without knowing the scale of security system being executed by the good nodes. Hence, in order to resist any possibility of being getting captured in the security system, the harmful node just mimick the behaviour of the good node for the malicious purpose of maximizing their trust factor. However, they do not continue doing it for long time as their energy will get unnecessary used in such task which is basically meant for initiating an attack. The proposed system implements the concept of sequential rationality where both harmful as well as good node are given equal chances to execute their actions.

The proposed system offers solution to this by performing security monitoring of the neighboring devices for two purpose i.e. vulnerability analysis and legitimacy analysis. In vulnerability analysis, the proposed system performs computation of trust factor which is based on observing and applying probability theory viz. probability that the computing good / harmful node will transmit the data packet to the next relay node, or drop it on the way, probability that the malicious node will help in transmitting the data packet to other good relay node or launch an attack. Hence, there are many probability factors that are actually computed in order to finalize the trust value that ultimately confirm the vulnerability of the targeted node. Legitimacy analysis basically deals with comparing the trust value obtained from the vulnerability analysis with the cut-off score of the trust value. If the computed trust value is found below some limit than based on it, it is confirmed to be good node or harmful node. One interesting part of the analysis is that if the good node declares another good node to be harmful node than the proposed sysem penalizes the prior good node. Hence, it makes sure that a good node always performs correct identification of the harmful node which increases the accuracy level of the detection. As a part of prevention tactic, the proposed system allocates reward for the good nodes and penalty for the harmful nodes.

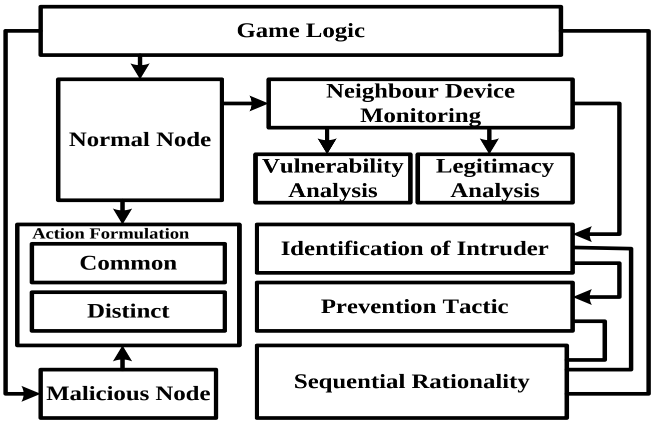

Fig.2 Block diagram for First Implementation Module

D. Integrated Model for Bandwidth Optimization and Energy Efficiency

This is the second module of implementation of the proposed system which targets to preserve channel capacity as well as retention of significant amount of energy efficiency. Fig.3 highlights the block diagram of this part of implementation where the initial part of design is to develop preliminary parameters of IoT viz. number of the communicating devices that are configured in specific deployment region, configurational setting for the gateway node that will carry out translational services. The next block is responsible for performing optimization operation towards the channel capacity of dynamic order. This operation is carried out by three sub-core components e.g. allocation gap time, effective capacity, as well as design of the scheduler. Finally an energy-efficient protocol is developed where the group-based communication is carried out with configured priority level.

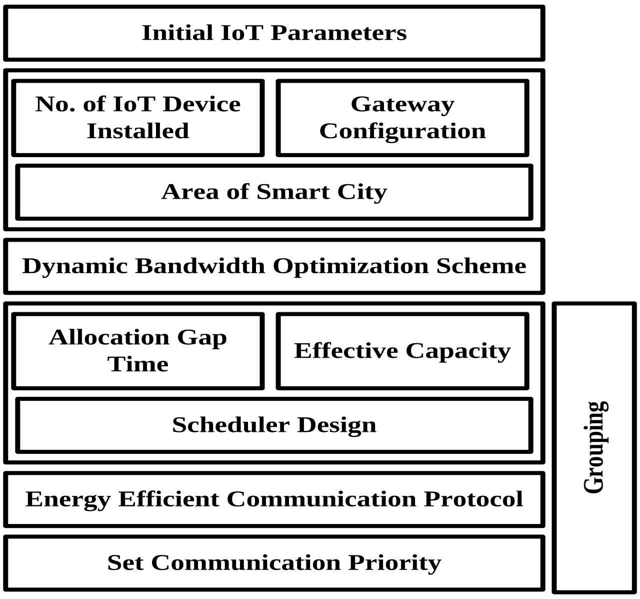
Initial IoT Parameters
No. of IoT Device Installed
Gateway Configuration
Area of Smart City
Dynamic Bandwidth Optimization Scheme
Allocation Gap Time
Effective Capacity
Scheduler Design
Energy Efficient Communication Protocol
Set Communication Priority
Grouping

Fig. 3 Block Diagram of Second Implementation Module

The proposed system carries out group-based communication system for all the communicating devices to the gateway node. This communication is facilitated by multihop-based approach where a memory is maintained for storing list of all the routes that leads to the gateway node at last.

The proposed system performs the optimization of the bandwidth with an aid of task provisioning scheme. The study considers two types of internal messages for communication where the first type of message is used for generating request and complying with the request while the second type of the message is used for `carry and transmiting the original data packet. The proposed system also make use of the priority indexing mechanism for the internal messages so that important data packets are always give increased priority over the conventional queue system that can further reduce delay as well as optimize the traffic performance too. The complete queue structure is redefined on the basis of the assigned level of priority. The most essential part of this phase of implementation is the energy efficiency model where the strategy is – all the communicating devices are identified first and then when they encounter a state of passiveness the proposed system turn off the receiving sensed signals from the radio of the communication devices. Once, the system ensures achieving the saturation point, the communicating devices roll back their mode to operational state and by doing so a significant amount of energy has been preserved. As per the logic implemented in the proposed system, the computation of the necessary energy is carried out by the source communicating device that is required for forwarding data and this computation of energy is carried out by the computing devices only after it receives a confirmation message. The dependable parameters in the computation of the energy are basically highest score of energy needed and threshold energy.

One interesting fact to be observed in the proposed implementation scheme is that it offers higher ranges of flexibility where both ongoing communication as well as optimization operation is carried out at same time. The operation of silencing the radio is only carried out after a definitive state of significant communication is identified. Hence, all the nodes need not to be in active state just to perform communication. Therefore, a significant amont of resources are reserved in this approach. At the same time, utilization of the channel capacity is significantly mainly due to provisioning scheme implemented in proposed system. The next section discusses about the results obtained after implementation.

III. RESULT ANALYSIS

The analysis of the proposed system is carried in simulation-based approach considering 500-600 communicating IoT devices that are spread over the simulation area of 1100x1200m^2 while assessment is carried out for 600 rounds of simulation. The analysis is carried out with respect to both the related approach of definitive technique [31] and probability allocation [32]. The performance is assessed with respect to probability of correct identification of malicious node and average vulnerability factor.

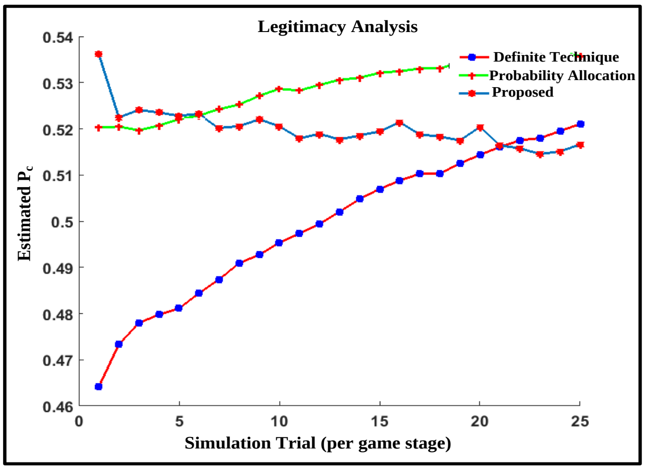

Fig.4 Comparative Analysis of Legitimacy

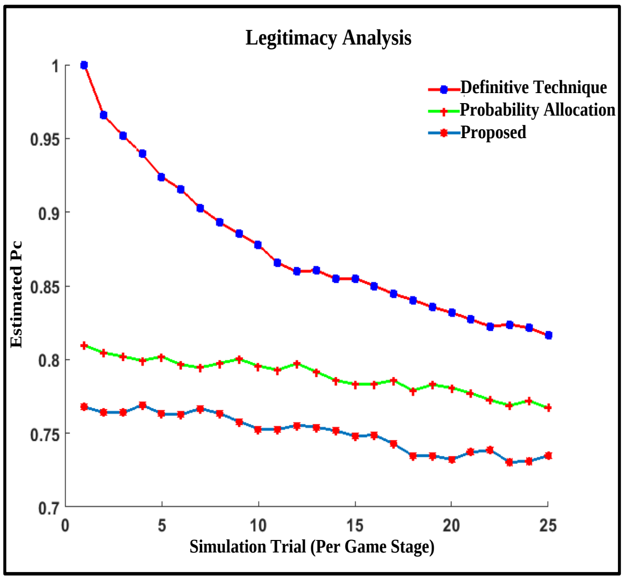

Fig.5 Comparative Analysis of Vulnerability

Fig.4 highlights the proposed system offers better consistency in identification of the malicious node while the other two approaches are found to be quite fluctuating performance with the increase of the simulation trials over each stage of the games. The prime reason behind this consistence factor is that proposed system computes probability of intrusion and this probability value is assessed and updated twice to reconfirm which leads to better accuracy and hence less fluctuation in outcome. Fig.5 highlights the mean vulnerability score as a result of the outcome which shows that vulnerability score is significantly reduced to greater extent as compared to existing security approaches. The interesting factor of the proposed outcome shows that without usage of any form of encryption, the proposed system offers significant resistivity against the potential threats in the distributed environment.

The next part of the analysis discusses about outcome of the energy efficiency as well as delay obtained from the proposed study. For this purpose, the proposed system considers REL protocol [33] as an existing system as a standard communication scheme in IoT environment.

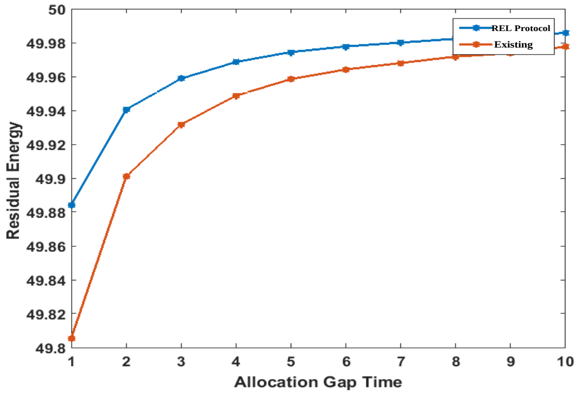

Fig.6 Comparative Analysis of Residual Energy

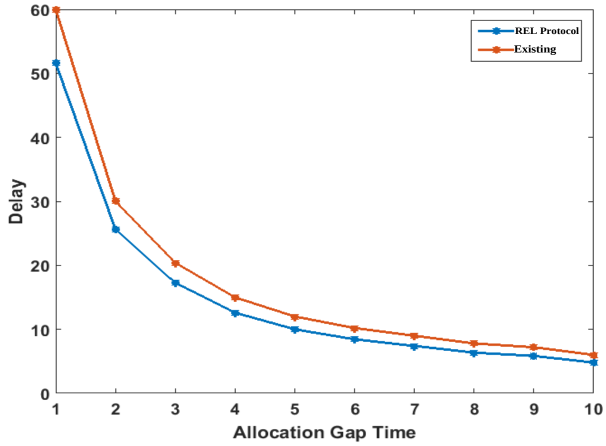

Fig.7 Comparative Analysis of Delay

It is eventual that energy will be dissipating with the increase value of the allocation gap time. Basically allocation gap time is distance between transmissions of two set of data packets to be forwarded. Fig.6 highlights that proposed system offer better retention of energy as compared to existing protocols while it also reduces delay (Fig.7). The prime reason behind this is adoption of proposed scheme allows a significant utilization of the channel capacity as well as energy efficiency in such a way that decision of forwarding data packets need not to be waited longer. This results in faster dissipation of informative contents from the communication nodes to IoT gateway nodes. Hence, the proposed system offers cost-effective solution towards energy efficiency, security, and bandwidth optimization.

IV. CONCLUSION

Developing a potential architecture for IoT system with full-fledge supportabilty towards futuristic sophisticated application is highly complex phenomenon. It is because of the reason that current state of commercial IoT application offers limites privileges and more shrouded with different technical challenges. This paper has addressed problems associated with security, bandwidth optimization, and energy efficiency which are the root causes of many other associated problems in IoT. The contribution made in this research work are as follows: i) the proposed system introduces a security system without using any encryption mechanism which is very much unconventional and yet it is capable of identifying and resisting malicious behavior of adversaries, ii) for a given set of channel capacity, the proposed system is capable of optimizing the performance of channel capacity due to new scheduling approach, and iii) the proposed system is also energy efficient as it doesn't apply any iterative and computationally complex process which ensures that proposed logic is highly applicable in practical environmental implementation.

REFERENCES

1. Fortino, Giancarlo, Antonio Guerrieri, Wilma Russo, and Claudio Savaglio. "Integration of agent-based and cloud computing for the smart objects-oriented IoT." In *Proceedings of the 2014 IEEE 18th international conference on computer supported cooperative work in design (CSCWD)*, pp. 493-498. IEEE, 2014.
2. Rosenkranz, Philipp, Matthias Wählisch, Emmanuel Baccelli, and Ludwig Ortmann. "A distributed test system architecture for open-source IoT software." In *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, pp. 43-48. ACM, 2015.
3. Datta, Soumya Kanti, Christian Bonnet, Amelie Gyrard, Rui Pedro Ferreira Da Costa, and Karima Boudaoud. "Applying Internet of Things for personalized healthcare in smart homes." In *2015 24th Wireless and Optical Communication Conference (WOCC)*, pp. 164-169. IEEE, 2015.
4. Samuel, S. Sujin Issac. "A review of connectivity challenges in IoT-smart home." In *2016 3rd MEC International conference on big data and smart city (ICBDSC)*, pp. 1-4. IEEE, 2016.
5. Bekara, Chakib. "Security issues and challenges for the IoT-based smart grid." *Procedia Computer Science* 34 (2014): 532-537.
6. Kumar, Nallapaneni Manoj, and Pradeep Kumar Mallick. "Blockchain technology for security issues and challenges in IoT." *Procedia Computer Science* 132 (2018): 1815-1823.
7. Bhandari, Rupesh. "Enhanced encryption technique for secure iot data transmission." *International Journal of Electrical & Computer Engineering (2088-8708)* 9 (2019).
8. Priyadharshini, S. G., C. Subramani, and J. Preetha Roselyn. "An IOT based smart metering development for energy management system." *International Journal of Electrical & Computer Engineering (2088-8708)* 9 (2019).
9. Pramukantoro, Eko Sakti, and Husnul Anwari. "An Event-Based Middleware For Syntactical Interoperability In Internet Of Things." *International Journal of Electrical and Computer Engineering* 8, no. 5 (2018): 3784.
10. Ambore, Bhagyashree, and L. Suresh. "Integrated Model of Bandwidth Optimization and Energy Efficiency in Internet-of-Things." In *Proceedings of the Computational Methods in Systems and Software*, pp. 379-388. Springer, Cham, 2019.
11. Alsaryrah, Osama, Ibrahim Mashal, and Tein-Yaw Chung. "Bi-objective optimization for energy aware internet of things service composition." *IEEE Access* 6 (2018): 26809-26819.
12. Bhattarai, Sulabh, and Yong Wang. "End-to-end trust and security for Internet of Things applications." *Computer* 51, no. 4 (2018): 20-27.
13. Bisadi, Mona, Alireza Akrami, Saeed Teimourzadeh, Farrokh Aminifar, Mehdi Kargahi, and Mohammad Shahidehpour. "IoT-Enabled Humans in the Loop for Energy Management Systems: Promoting Building Occupants' Participation in Optimizing Energy Consumption." *IEEE Electrification Magazine* 6, no. 2 (2018): 64-72.
14. Caruso, Antonio, Stefano Chessa, Soledad Escolar, Xavier Del Toro, and Juan Carlos López. "A dynamic programming algorithm for high-level task scheduling in energy harvesting IoT." *IEEE Internet of Things Journal* 5, no. 3 (2018): 2234-2248.
15. Ju, Qianao, Hongsheng Li, and Ying Zhang. "Power management for kinetic energy harvesting iot." *IEEE Sensors Journal* 18, no. 10 (2018): 4336-4345.
16. Casado-Mansilla, Diego, Ioannis Moschos, Oihane Kamara-Esteban, Apostolos C. Tsolakis, Cruz E. Borges, Stelios Krinidis, Ane Irizar-Arrieta et al. "A human-centric & context-aware IoT framework for enhancing energy efficiency in buildings of public use." *IEEE Access* 6 (2018): 31444-31456.
17. Shafique, Kinza, Bilal A. Khawaja, Muhammad Daniyal Khurram, Syed Maaz Sibtain, Yazir Siddiqui, Muhammad Mustaqim, Hassan Tariq Chattha, and Xiaodong Yang. "Energy harvesting using a low-cost rectenna for Internet of Things (IoT) applications." *IEEE Access* 6 (2018): 30932-30941.

18. Roy, Swati Sucharita, Deepak Puthal, Suraj Sharma, Saraju P. Mohanty, and Albert Y. Zomaya. "Building a sustainable Internet of Things: Energy-efficient routing using low-power sensors will meet the need." *IEEE Consumer Electronics Magazine* 7, no. 2 (2018): 42-49.
19. Zhai, Daosen, Ruonan Zhang, Lin Cai, Bin Li, and Yi Jiang. "Energy-efficient user scheduling and power allocation for NOMA-based wireless networks with massive IoT devices." *IEEE Internet of Things Journal* 5, no. 3 (2018): 1857-1868.
20. Mozaffari, Mohammad, Walid Saad, Mehdi Bennis, and Mérouane Debbah. "Mobile unmanned aerial vehicles (UAVs) for energy-efficient Internet of Things communications." *IEEE Transactions on Wireless Communications* 16, no. 11 (2017): 7574-7589.
21. Ji, Wen, Jingce Xu, Hexiang Qiao, Mengdi Zhou, and Bing Liang. "Visual IoT: Enabling Internet of Things Visualization in Smart Cities." *IEEE Network* 33, no. 2 (2019): 102-110.
22. Lee, Byung Moo. "Multi-Point Media Content Sharing Scheme in Internet of Things Networks." *IEEE Access* 6 (2018): 71360-71367.
23. Cao, Haotong, Longxiang Yang, and Hongbo Zhu. "Novel node-ranking approach and multiple topology attributes-based embedding algorithm for single-domain virtual network embedding." *IEEE Internet of Things Journal* 5, no. 1 (2017): 108-120.
24. Hou, Weigang, Wenxiao Li, Lei Guo, Yiwei Sun, and Xintong Cai. "Recycling edge devices in sustainable Internet of Things networks." *IEEE Internet of Things Journal* 4, no. 5 (2017): 1696-1706.
25. Kua, Jonathan, Suong H. Nguyen, Grenville Armitage, and Philip Branch. "Using active queue management to assist IoT application flows in home broadband networks." *IEEE Internet of Things Journal* 4, no. 5 (2017): 1399-1407.
26. Hou, Zhanwei, He Chen, Yonghui Li, and Branka Vucetic. "Incentive mechanism design for wireless energy harvesting-based Internet of Things." *IEEE Internet of Things Journal* 5, no. 4 (2017): 2620-2632.
27. Huang, Xumin, Rong Yu, Jiawen Kang, Zhuoquan Xia, and Yan Zhang. "Software defined networking for energy harvesting internet of things." *IEEE Internet of Things Journal* 5, no. 3 (2018): 1389-1399.
28. Javed, Abbas, Hadi Larijani, and Andrew Wixted. "Improving Energy Consumption of a Commercial Building with IoT and Machine Learning." *IT Professional* 20, no. 5 (2018): 30-38.
29. Long, Nguyen Bach, Hoa Tran-Dang, and Dong-Seong Kim. "Energy-aware real-time routing for large-scale industrial internet of things." *IEEE Internet of Things Journal* 5, no. 3 (2018): 2190-2199.
30. Moghaddam, Mohammad Hossein Yaghmaee, and Alberto Leon-Garcia. "A fog-based internet of energy architecture for transactive energy management systems." *IEEE Internet of Things Journal* 5, no. 2 (2018): 1055-1069
31. A. Agah, S. K. Das and K. Basu, "A game theory based approach for security in wireless sensor networks," IEEE International Conference on Performance, Computing, and Communications, 2004, 2004, pp. 259-263.
32. M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 920-925.
33. Kassio Machado, Denis Rosario, Eduardo Cerqueira, "A Routing Protocol Based on Energy and Link Quality for Internet of Things Applications", Open-Access Sensors, vol.13, pp.1942-1964, 2013

AUTHORS PROFILE

Bhagyashree Ambore, completed her B.E in Computer Science and Engineering in 2006 and M.Tech in Computer Science and Engineering in 2012 and awarded as “young Investigator”. Currently she is pursuing her PhD in computer science and Engineering from Visvesvaraya Technological University. She is working as Assistant Professor in the Department of Computer Science and Engineering at Cambridge Institute of Technology, Bangaluru. She has more than 7 years of experience in teaching.

Suresh L Obtained, his B.E degree in Computer Science and Engineering from GIT Belagum, Karnataka University in 1990 and M.E in Computer Science and Engineering in St. Peter’s University, Chennai. He received Ph.D degree in Computer Science and Engineering in 2010. Right from 1990 he is working in the Department of Computer Science & Engineering under various designations. Presently he is working as Principal and Professor in Department of Computer Science and Engineering at Cambridge Institute of Technology, Bengaluru. He has more than 28 years of experience.