International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 54, No. 2, April, 2021, pp. 229-233
Journal homepage: http://iieta.org/journals/jesa

Advanced System Control with Traffic Handling for Secure Communication in IoT Routing Protocol

Kurra Santhi Sri[1*], Komanduri Venkata Sesha Sai Rama Krishna[2], Venkata Bhujanga Rao Madamanchi[3], Gondi Yasoda Devi[4]

[1] Department of IT, Vignan's Foundation for Science, Technology and Research, Guntur 522213, Andhra Pradesh, India
[2] Department of CSE, Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur 522009, Andhra Pradesh, India
[3] Dept. of Information Technology, RVR & JC College of Engineering, Guntur 522019, Andhra Pradesh, India
[4] Department of CSE, GITAM Institute of Technology, GITAM (Deemed to be University), Visakhapatnam 530045, Andhra Pradesh, India

Corresponding Author Email: kurrasanthisri4@gmail.com

https://doi.org/10.18280/jesa.540204

Received: 18 June 2020
Accepted: 26 March 2021

Keywords:
traffic handling, secure communication, IoT routing protocol, system control, access control

ABSTRACT

The Internet of Things (IoT) can simply be referred to as the network of things comprising software, sensors, electronics, allowing data to be collected and transmitted. The next step in the field of technology is the Internet of Things, bringing tremendous improvements to manufacturing, medicine, environmental treatment, and urban growth. In shaping this vision, multiple challenges need to be faced, such as technology interoperability problems, protection and data confidentiality standards and, last but not least, the implementation of energy efficient management systems. These devices with minimal human interference are capable of producing, sharing and consuming data. The networking of related as well as heterogeneous devices is often known to be IoT. The Internet of Things allows things to connect and interact with each other, thus minimizing human involvement in simple daily tasks. Addressing protection at all times or at any position for many users, companies, governments, and enterprises is really necessary and responsive. In this paper a secure IOT architecture for routing in a network with RPL Rapid Node Link Routing (RNLR) Model is proposed that performs traffic management and traffic analysis for secure communication using IoT routing protocol. It mainly aims to locate the malicious users in a IOT routing protocols. the proposed mechanism is compared with the state of the art work and compared results shows the proposed work performs well.

1. INTRODUCTION

The Internet of Things referred to as the full system of data collection, sensors and electronics [1]. The Internet of Things is the cloud. IoT applications include intelligent homes and communities, connected vehicles, hospitals, smart farming, the industrial internet, growth, and smart retail. Increasing business discomfort, improving efficiency, improving living quality and being very productively, IoT offers many benefits by saving time and time [2]. IoT provides a safer environment for communication. There are many disadvantages in IoT, in addition to advantages: lower protection of data and low security, usability and technological dependency. Protection in IoT is the main problem and obstacle [3].

In IoT, routing is a key factor which makes it easy to link devices and transmit data. The introduction of a good routing protocol will improve the efficiency of the LLNs [4] networks. In order to define the efficiency of a protocol, we can use factors such as energy consumption, overall management, delivery ratio, latency. The IoT IPV6 network [5] is a key component of routing. The IoT will become true with the Routing Protocols.

The goal of this study is to use IoT, agents and other technologies to improve traffic conditions and alleviate traffic pressure. Travelers and other users can be provided with information created by IoT traffic and collected on all roads. The scheme will identify current traffic operations, traffic flow patterns and conditions from collected real-time traffic data. It can forecast the future flow of traffic. Some may be provided by the framework. The latest details on real-time traffic that lets drivers choose Optimal itineraries [6]. The device will, therefore, effectively administer, track and control moving vehicles. The basic IoT architecture is indicated in Figure 1.

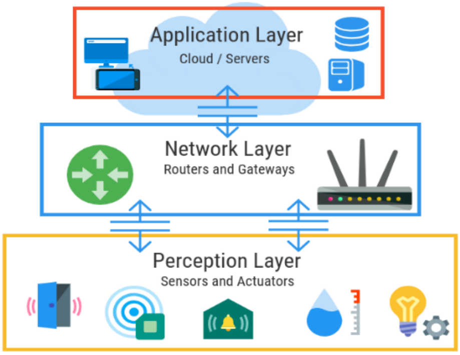

Figure 1. Basic IoT three layer architecture

The development of an intelligent IoT traffic system offers various advantages, such as improving conditions for traffic, minimizing traffic jams and management costs, ensuring high reliability, shielding traffic and freeing it from weather [7]. The defense by IoT traffic should be extended to all aspects of traffic, including highways, bridges, tunnels, traffick signals, cars and drivers [8]. All of this will be connected to the Internet in order to easily recognize and control by sensor devices, such as RFID devices, infrarot sensors, international positioning systems, laser scanners, etc. The Traffic IoT offers information collection and integration for the automated and intelligent processing of all forms of information on large-scale roads. This turns modern traffic control into a smart IoT system [9].

Smart infrastructure is an important aspect of smart city initiatives because traffic jamming and population development are a serious issue [10]. Smart transport systems are used in intelligent traffic control systems with integrated components [11], and roadside units [12]. These systems collect traffic data in real-time and take the appropriate steps to prevent or mitigate any social problems caused by road congestion [13]. Links to real-time traffic maps, for instance, can help residents choose suitable routes to save time and effort. The list of attacks that are considered to be secure is Sybil Attack: This is the type of attack in which, by establishing multiple identities, the integrity of the node is subverted [14].

Sinkhole Attack: Sinkhole attack is carried out in the network by either hacking nodes and adding corrupted or produced nodes. By providing false facts, the intruder node or sinkhole node diverts the traffic towards itself from other nodes. The node information was thus easily exploited by attacker nodes. The effect of the Sinkhole attack is further power consumption [15].

Sleep Deprivation Attack: The attack where victim nodes remain awake, resulting in more battery use, is the attack of sleep deprivation. It decreases the lifespan of the cell, causing the nodes of the victim to shut down.

Denial of Service Attack: In this attack, hackers overload the IoT network with unwanted traffic signals, resulting in service not always available.

Injection of malicious code: In this attack, the hacker adds the compromised node by entering the system's validation vulnerability to insert malicious code. This results from the network being shut down or an intruder taking complete control of the network.

Man-in-the-Middle Attack: In this attack, either by secretly eavesdropping or manipulating the traffic signals to track and manipulate the private conversation, the attacker intercepts the correspondence between two nodes, resulting in information leakage, identification, much more.

2. RELATED WORK

Al-Fuqaha et al. [1] proposed rank assault in nature distracts gradually and the attacker node can insist on the routing of its neighboring protocols in LLN systems to route information via their power without the use of much stretching power. In addition, the results showed that, depending on the situation of the attacker node within the network, a proposed attack could decrease 30% – 57% of the share of data transmission.

The storage mode or storage mode may be used with each node in the RPL. In the storage mode, the node will receive and transfer the data to its parent node. The node transfers the data in non-storage mode to its parent node. The RPL promotes traffic patterns, such as points, points, points and points [16-18]. The RPL promotes traffic patterns.

A sigma routing metric for RPL has been proposed by Han et al. [3]. Large-scale networks do not support the current objective functions based on the RPL protocol. Network size increases as the hop count increases, it is noted. Thus, the bottleneck issue is created closer to the DODAG core. The proposed objective function utilizes the standard deviation of the ETX value to pick an ideal parent for data transfer in order to solve this problem. The simulation is performed using the simulator COOJA.

A drizzle algorithm for preserving the route information in LLN has been proposed by Aanchal Khatri et al. [4]. This solves the trickle timer problem in the standard RPL. The control message is suppressed by the Drizzle trickle timer, as it assigns a different probability value to each node in the network. It thus improves the efficiency of the network during the selection and maintenance of routes. The drizzle algorithm, as it omits the listen-only duration, increases the convergence time. The simulation is performed using the simulator COOJA. The outcome of the simulation shows that the efficacy of drizzle-RPL is assessed under various network conditions and compared to RPL and MHROFRPL.

A smart home threat model was introduced and analyzed in the IoT application by Geneiatakis et al. They showed that in the threat model, the smart home is vulnerable to attacks by eavesdropping, impersonation, Denial of Service (DoS) and software manipulation. The model of the authors considers two types of attacks, namely: internal within the premises of the smart home and external entities that interfere with the Internet connection. Santoso and Vun, on the other hand, presented a new approach to introduce a Wi-Fi network-based smart home system.

Khatri et al. [5] "A Selective Forwarding Attack Intrusion Detection System in IPv6-based Mobile WSNs" This paper focuses primarily on the detection of selective forwarding intruders, the proposed IDS-based solution is to find a selective forwarding attack that also removes modified nodes, the proposed IDS improves great efficiency within the mobile network at the expense of overhead control.

Airehrour et al. [7] "Implementation of a Wormhole Attack Against an RPL Network: Challenges and Effects" Framed an attack by giving a wormhole execution as opposed to IEEE 802.15.4 WSAN. On a genuine RPL topology, the proposed attack was implemented. The studies suggested that the proposed attack could be convincing to undergo a different attack such as a DoS. We ended up exploring the prospect of conceivable countermeasures in the long run.

Ahmed et al. [9] In order to reduce sybil attacks with RPL mobility, Order suggested a trusted IDS (T-IDS) solution to minimize RPL mobility sybil attacks. As RPL is subject to sybM, overhead control and energy usage have increased, and the delivery ratio of packets has been decreased. The T-IDS proposed tackles the problems resulting from RPL symbolic mobility attacks.

Atakli et al. [13] "Securing Blackhole Attacks RPL Routing Protocol using Trust-based Mechanism" This document introduced a new trusted, trustworthy routing protocol to provide a feedback-conscious trust based protection framework for IoT systems. This system represents a value (trust) for the nodes that rely on the broad sending behavior of neighboring hub models. As seen in the trust value performance, knowledge feedback will be presented among the nodes and the trust evaluation will also be checked.

3. PROPOSED WORK

The proposed model expects the client to decide which router(s) the monitor(s) fills in, but for this reason it is not clear how to choose the router(s). To choose a relevant monitor, analysis had to be performed on the nodes involved in communication and their behaviour was analyzed.

The main aim of traffic signal control is to maximize the use of intersection efficiency and to satisfy intersection transportation needs. Vehicle delay is an important parameter for calculating traffic signal control in order to extract data from each module and minimize the average delay by using the required adaptive genetic algorithm due to road conditions. The improved approach is used to minimize the limitations of conventional genetic algorithms in terms of convergence and the potential to maximize global optimization.

Algorithm for working of router in RPL Rapid Node Link Routing

Step 1: Input the nodes in the network
Step 2: Consider a node as a DIO
Step 3: Enable Validation for DIO node and check status

```
    If validated
        Calculate the rank of the DIO node
        If rank is in range then share the message to other nodes in the network
        rank(DIO)=rank(parentNode)+(rank++);
    If validation fails
            Re perform validation process
        If validated
            Calculate the rank of the DIO node
            If rank is in range, then share the message to other nodes in the network
            rank(DIO)=rank(parentNode)+(rank++);
        If validation fails
        Mark the node as malicious and label it to avoid entering into network.
```

Step 4: Calculate the trust factor of each node in the network after validation as

$$\sum_{i=1}^{N} N(i) = \sum_{i=1}^{N} rank_i\,(w_i.N_i + \mathrm{Th})$$

Step 5: Identify the neighbor node ID and perform DIO node validation on all the neighbors for established the secure route.
Step 6: For every neighbor node, calculate the rank of the node and compare it to DIO node for fixing the node in the routing process. The process if performed as

```
foreach N(i) ∈ net(DIO)
for each instance i ∈ N
do
|W(N(i))| ← W (I1, I2 ∈ N), I1 & I2 are neighbor nodes and W the weight of the node for giving priority to update in the routing process is calculated as:
```

$$W(N_{i,j}) = \frac{2T_j^{(C_i)}}{|N(W)_j|}$$

Step 7: Update the routing information
Step 8: End

The traffic load is determined between source node N to the DODAG node on path T calculated as:

$$TrafficLoad\left(Ni_{,DODAG\ \ root}\right) = \sum_{x=1}^{T} Load\,(r) + T(N(i))$$

Here N is the total nodes in network and r is the initial node considered. The traffic on a particular node is calculated as:

$$trafficLoad\,(r) = \sum_{i=1}^{N} child - count(N) + DIO(N)$$

The amount of energy consumed at each node in routing process is calculated as:

$$Ene(N(i)) = \frac{\sum_{i=1}^{T} Tn_i}{trafficLoad(r)}\left(e_r + (e_t \times dis)\right)$$

where, er is the energy released and et is energy used in the network by a node. The route optimization is performed as:

$$R1 = e_8 + (e_t \times dis) + \frac{\sum_{t=2}^{T} pn_t}{gt}(e_r + (e_t \times dis))$$

$$R = R1 +_2 \times \left(\frac{1}{2}r\right)^N + P + w(i) \times \frac{N^i - r^2}{r^2}$$

4. EXPERIMENTAL RESULTS

Using the COOJA network simulator, the proposed protocol was assessed and compared to familiar routing protocols such as FL-RPL. There is one DODAG root node with a hundred RPL routers in the simulation. In three cases, the simulation is carried out with a data transfer rate of one, six and ten packets per minute. The average values obtained during the simulation are given as the outcomes. The Table 1 shows the parameters for simulation setting.

Table 1. Parameters for Simulation

Parameter	Value
OS	Contiki 2.7
Simulator	COOJA
Min DIO Interval	12
Node Type	Tmote sky
Network Area	600 X 600
RPL Parameter	minHopRankIncrease=256
Battery	1500 mA
Simulation Time	60 Min
Data Packet Time	30 Sec

Network performance is defined as the rate of effective packet transmission through a network channel. Thus, we can sum up all the packets obtained for small networks in order to calculate the value. There are several ways to measure the (instant or average) performance of a wired or wireless network with the aid of network simulators. Figure 2 shows the simulation model for an IoT network.

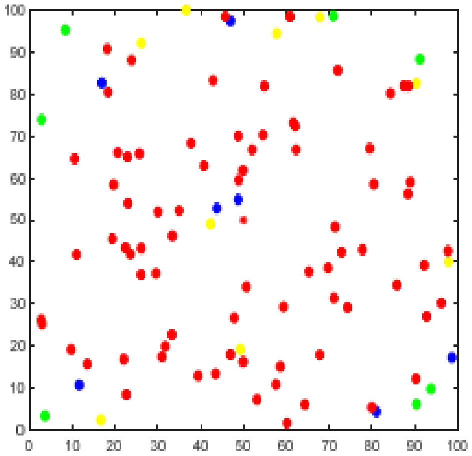

Figure 2. Simulation network

Simply set the PDR Packet Delivery Rate as the ratio between the packets produced and the packets received. The difference between the sender time when the packet was produced and the received packet. End-to-end delays are also considered a means to prolong the time it takes to transfer a packet from sender to recipient over the network.

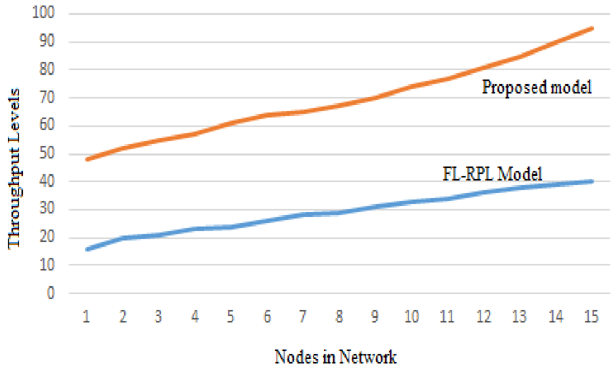

Figure 3. Throughput levels

Figure 3 shows the efficiency relation between the normal RPL, the new secure RPL and our proposed mechanism. The regular RPL protocol has the most recent and proposed performance, but it is very close to standard RPL and more dominant than established work.

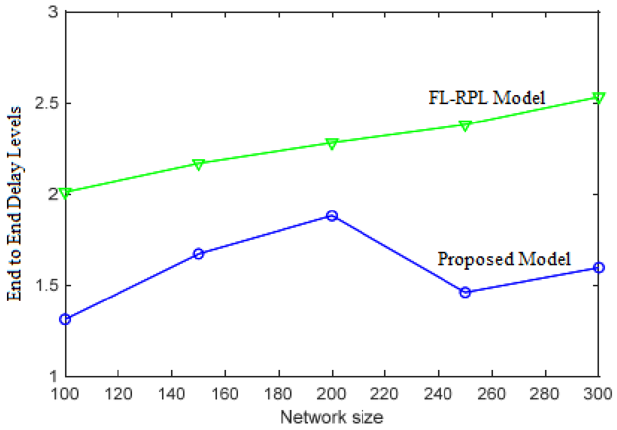

Figure 4. Delay levels

Figure 4 offers a comparison of end-to-end delays between the traditional RPL protocol, the latest protective RPL and the mechanism we have proposed. The standard RPL Protocol has a very low delay compared to the current one and the proposed one, but the proposed delay is close and dominant than the current work and the conventional RPL.

Figure 5 provides a contrast between the RPL protocol, the new stable RPL and our proposed mechanism for packet delivery. The usual RPL protocol is higher than what is currently in place and suggested, but it is still similar to the traditional RPL and is more prevalent than work already carried out. The proposed model takes into account the performance levels of the attacking nodes, and the safety criteria are shown in Figure 6.

The end to end delay of the model by considering attacker nodes in the network is represented in Figure 7.

The proposed model performs traffic management and traffic analysis and the time levels for traffic analysing is indicated in Figure 8. The proposed model takes less time for analysis of traffic and performs traffic management accurately. The Figure 8 indicates the time levels for traffic analysis.

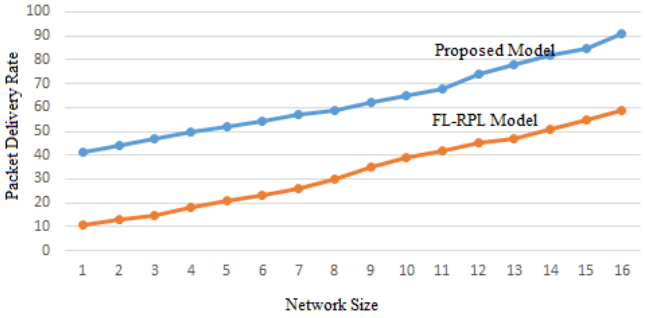

Figure 5. Packet delivery rate levels

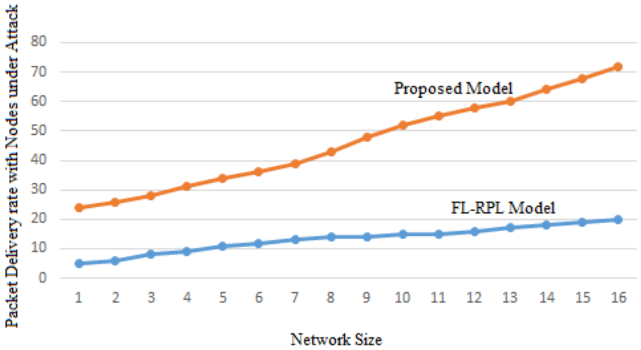

Figure 6. Packet delivery rate with nodes under attack

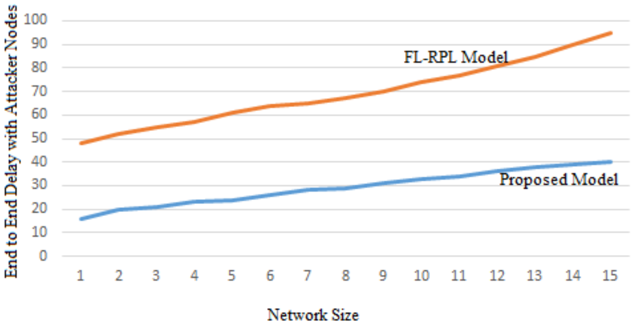

Figure 7. End to End Delay with attacker nodes

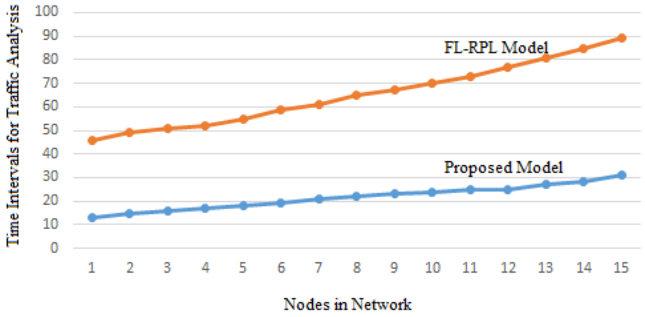

Figure 8. Time intervals for traffic analysis

5. CONCLUSION

The Internet of Things (IoT) has progressed its global pervasiveness with the goal of developing intelligent networks. It aims to build the network edge for the use of intelligent services and computing through IoT devices. Safe communication is a key feature in any type of network. IOT is a very large network and secure communication is very difficult. In order to route, the IOT proposes many routing protocols. However, most of them have secure touch. This paper focuses mainly on secure communication between different IOT nodes, in order to identify malicious Nodes and secure communication via a network monitoring based process. The proposed mechanism is effective, in contrast to literary mechanisms. Each of the objects in the future Internet of Things (IoT) network communicates with other objects and acquires personal data. The energy efficiency of the nodes is essential to the performance of the network in distributed IoT networks.

REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4): 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

[2] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7): 1645-60. https://doi.org/10.1016/j.future.2013.01.010

[3] Han, G.J., Jiang, J.F., Shu, L., Niu, J.W., Chao, H.C. (2014). Management and applications of trust in wireless sensor networks: A survey. Journal of Computer and System Sciences, 80(3): 602-617. https://doi.org/10.1016/j.jcss.2013.06.014

[4] Aanchal, Kumar, S., Kaiwartya, O., Abdullah, A.H. (2017). Green computing in wireless sensor networks: Huffman coding and optimization approach. Peer-to-Peer Networking and Applications, Springer, 10: 592-609. https://doi.org/10.1007/s12083-016-0511-y

[5] Khatri, A., Kumar, S., Kaiwartya, O. (2017). Towards green computing in wireless sensor networks: Controlled mobility aided balanced tree approach. International Journal of Communication Systems, 31(7). https://doi.org/10.1002/dac.3463

[6] Khatri, A., Kumar, S., Kaiwartya, O. (2016). Optimizing energy consumption and inequality in wireless sensor networks using NSGA-II. In Proceedings of ICCCS, Taylor & Francis, https://doi.org/10.1201/9781315364094-66

[7] Airehrour, D., Gutierrez, J., Ray, S.K. (2016). Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66: 198-213. https://doi.org/10.1016/j.jnca.2016.03.006

[8] Feng, R., Xu, X., Zhou, X., Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. Sensors, 11(2): 1345-1360. https://doi.org/10.3390/s110201345

[9] Ahmed, A., Bakar, K.A., Channa, M.I., Haseeb, K., Khan, A.W. (2015). Terp: A trust and energy aware routing protocol for wireless sensor network. IEEE Sensors Journal, 15(12): 6962-6972. https://doi.org/10.1109/JSEN.2015.2468576

[10] Kaiwartya, O., et al. (2018). Virtualization in wireless sensor networks: Fault tolerant embedding for Internet of Things. IEEE Internet of Things Journal, 5(2): 571-580. https://doi.org/10.1109/JIOT.2017.2717704

[11] Huang, J., Meng, Y., Gong, X., Liu, Y., Duan, Q. (2014). A novel deployment scheme for green internet of things. IEEE Internet of Things Journal, 1(2): 196-205. https://doi.org/10.1109/JIOT.2014.2301819

[12] Feng, R., Che, S., Wang, X., Yu, N. (2013). Trust management scheme based on DS evidence theory for wireless sensor networks. International Journal of Distributed Sensor Networks, 9(6): 948641. https://doi.org/10.1155%2F2013%2F948641

[13] Atakli, I.M., Hu, H., Chen, Y., Ku, W.S., Su, Z. (2008). Malicious node detection in wireless sensor networks using weighted trust evaluation. Proceedings of the 2008 Spring simulation multiconference (pp. 836-843). Society for Computer Simulation International. https://doi.org/10.1145/1400549.1400686

[14] Chze, P.L.R., Leong, K.S. (2014). A secure multi-hop routing for IoT communication. 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea (South) pp. 428-432. https://doi.org/10.1109/WF-IoT.2014.6803204

[15] Rani, S., Talwar, R., Malhotra, J., Ahmed, S.H., Sarkar, M., Song, H. (2015). A novel scheme for an energy efficient Internet of Things based on wireless sensor networks. Sensors, 15(11): 28603-28626. https://doi.org/10.3390/s151128603

[16] Tyagi, S., Kumar, N. (2013). A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. Journal of Network and Computer Applications, 36(2): 623-645. https://doi.org/10.1016/j.jnca.2012.12.001

[17] Georgios, S., Matta, I., Bestavros, A. (2004). SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. Boston University Computer Science Department, 2004.

[18] Hussain, S., Matin, A.W. (2005). Energy efficient hierarchical cluster-based routing for wireless sensor networks. Jodrey School of Computer Science Acadia University Wolfville, Nova Scotia, Canada, Technical Report, (2005): 1-33.