Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 89 (2016) 218 – 227

Procedia
Computer Science

Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016)

A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT)

Carynthia Kharkongor*, T. Chithralekha and Reena Varghese

Pondicherry University, Pondicherry 605 014, India

Abstract

Internet of things is a new paradigm that aids the communication between heterogeneous devices and objects. It provides a unified framework that allows interoperability across varied platforms. It has the ability of sharing the information globally be it with any device. By 2020, it is estimated that nearly about 50 billion of devices will be connected. By providing an exclusive and unique identity for each object, gives the privilege for any device to connect to the internet. The main focus is to permit 'anyone' or 'anything' at 'any time' to exchange information services from 'anywhere' 'anyplace'. This emergence technology keeps the people connected with 'anything' and 'anyone' and be it 'anywhere'. To achieve this, routing protocol is needed that will entail the transmission of data between heterogeneous devices. In this paper, a routing protocol is proposed that will take in consideration the energy consumption of the heterogeneous devices. A SDN controller is also introduced in the network that serves as a centralized manager providing a secure network by denying access to selfish nodes that are present in the network.

Keywords: Internet of Things (IoT); Software Defined Network (SDN); SDN Controller; Open Flow.

1. Introduction

The word 'Internet' is the interconnection of networks linking millions of devices for exchanging information resources and services .The information is sent to any medium be it. 'Thing' can be any kind of object whether device, gadget or item[1]. The internet of things is a new technology that leads to the interconnection of objects and device at an unprecedented pace and scale. It has the concept of 'anything', 'anywhere' that entail the connectivity of any device or object. This way objects and devices stay connected to each other rather than people. The main aim of internet of things is the transmission of information through the internet without the aid of human intervention.[2] It will dramatically change the lifestyle of the people allowing more proactive behaviour of devices than reactive. The heterogeneous devices will expand into places that were unreachable back then. As Internet of Things (IoT) consist of vast heterogeneous networks that consist of different capacity, processing power and platform. In order to meet the above requirements, routing protocols are needed to aid in the intercommunication between the different devices[3].

In this paper, Section 2 explains the literature survey on different routing protocols. Section 3 brief describes the main issues in Internet of Things (IoT). Section 4 states the major problem relating to IoT and in Section 5, a new

*Corresponding author. Tel.: +91 -7598134083.
E-mail address: carynthiakharkongor@gmail.com

doi:10.1016/j.procs.2016.06.048

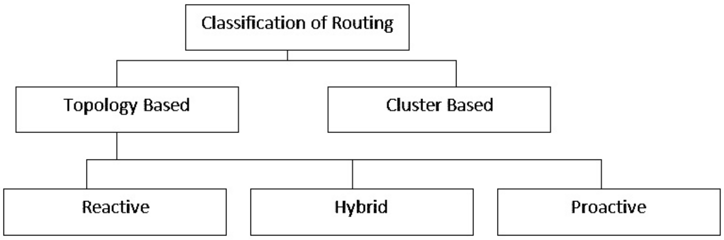

Fig. 1. Classification of Routing Protocols.

proposed routing is introduced with SDN controller that acts as a centralized controller. Section 6 shows the simulation of the proposed routing using NS-2 and Section 7 gives the analysis of the proposed routing and the comparison of the routing with the other routing protocols.

2. Literature Survey

2.1 Routing in the internet of things

Data transmission becomes an important for communication, be it human to human or human to machine or machine to machine interaction. Time plays a very important role in data transmission, so that the message will reach the destination in a permissible time period. Therefore the data should be routed in such a way that it will take the least or shortest path to reach the destination. Routing is the process of establishing and maintaining route between mobile modes in wireless networks. There are two types of routing protocols based on the criteria.

- Topology: refers to the arrangement of the nodes and objects in the network.
  There are three types of topology protocols. They are as follows:
  i. Reactive: the routes are created only when the source needs to send packets to the destination
  ii. Proactive: each node has complete information about the topology of the whole network
  iii. Hybrid: it is the combination of both reactive and proactive routing protocols.
- Clustering:
  It is one of the technique in which nodes are group into clusters. Each cluster will select a cluster head. The cluster head communicate with other cluster heads for transmitting the packet. This eventually saves the energy of the node as communication will occur via the cluster head[12].

2.2 Routing protocols

- *DSDV (Destination Sequence Distance Vector)*
  Each node has a routing table which contains all the available destination, number of hops and sequence number. These information are required in order to find the route to the destination node.
- AODV (Ad-hoc on demand distance vector)
  It is a development of the DSDV by creating paths on demand which, thereby reduces the number of broadcasts[4,6]. AODV uses different kind of control messages Route Request Message (RREQ) for sending request, Route Reply Message (RREP) for replying, Route Error Message (RERR) for checking error and Hello message to check whether the route is still alive[5,6].
- AOMDV (Ad-hoc on demand multipath distance vector)
  It is improved version of AODV designed to solve the problem of multipath[5]. It is suitable for highly dynamic network where link breakage occurs repeatedly. It contains a routing table which lists a series of hops along with the hop counts[6].

- LEACH (Low Energy Adaptive Clustering Hierarchy):
  This protocol is based on clustering technique where nodes are classified into different clusters with cluster head for each. The cluster head serves the process of transferring the data packets. It is selected by using a threshold value t(n) random number 0 or 1 will be selected by each node and then it is compared with the threshold value t(n).[7,8]
- WRP (Wireless routing protocol)
  It is a table based in which each node will have three tables such as a routing table that contains routing details, message retransmission list and link cost table that contains cost for each link in the route. Node exchanges their routing table with the neighbours using update message. The unique feature about this protocol is that it is able to check inconsistency whenever any changes occurs in the network which help to eliminate loop situations.[7]
- ZHRL (Zone-based Hierarchical Link State Routing Protocol)
  The nodes are partitioned in such a way that each node has two non – overlapping zones. They are node and zone level. Node level specifies how each node in the zone is connected to each other whereas zone level specifies how the zone is connected to each other. There are also two types of link state packets known as the zone and the other as non-zone link state packets. Node Link state packet contains information about its neighbour zone while zone link state packet contains information about the neighbour zone.[7]
- CGSR (Cluster Head Gateway Switch Routing Protocol)
  It is mainly developed on the basis of DSDV routing protocol. The network is being grouped into cluster of nodes with the cluster head in each group. The cluster head will transmit this packet to the gateway node. This algorithm uses the Least Cluster Change algorithm where the cluster head will be changed only when two cluster heads come into one cluster or one of the nodes will move out from the area of the two cluster heads[7].
- TORA (Temporally Ordered Routing Algorithm)
  TORA is based on the link reversal. The main functions of the protocol are: route creation, maintenance and erasure. Each node contains the following information such as the time in which the link fails, unique ID of the node, indicator bit for reflection and ordering parameter during propagation. The route creation has two packets: QRP & UPD packets[7].
- ABR (Associativity Based Routing)
  It defined a new metric known as the degree of association stability. A route will be created based on the associativity of the nodes in the network. To keep the network alive, beacons are sent. There are three phases in this protocol[7].
- SSR (Signal Stability Routing) protocol
  It selects the route for the packet based on the energy strength of the node and the node's location. It contains two types of protocol: dynamic routing protocol (DRP) and static routing protocol (SRP). The dynamic routing protocol has two tables: signal stability table and routing table. The signal strength table records the strength of the neighbouring nodes as weak or strong channel. All transmission are processed by DRP and passed to SRP after updating[7].
- FSR (Fisheye State Routing)
  FRS is an improved routing protocol of GSR. Instead of containing information about all the nodes, the update message will contain information about the neighbours. Even the nodes do not contain information about the other nodes but the packet will reach destination because the information will be more accurate as it reaches the destination[7].
- GSR (Global State Routing)
  It is an improved version of DSDV that avoids flooding of message. Each node in this protocol contains neighbour list, next hop table, distance table, topology table. The neighbour list contains list of the neighbours. Distance table contains shortest distance from each destination and next hop table contains next hop that packets needs to be forwarded to reach destination. When node receives routing message, it checks the sequence number. If it is less than available, then it is updated else it is discarded. Then it will broadcast this routing information to other neighbours[7].

Table 1. Comparison of the different Routing Protocols 6.

Parameters	AODV	DSDV	AOMDV	LEACH	WRP	ZHLP	CBGR	TORA	ABR	SSR	GSR	FSR
Types of Routing Used	Reactive	Pro-Active	Reactive	Cluster -based	Pro-active	Hybrid	Reactive	Reactive	Reactive	Reactive	Pro-Active	Pro-Active
Based on Topology	Flat	Flat	Flat	Hierarchical	Flat	Hierarchical	Hierarchical	Flat	Flat	Flat	Flat	Flat
Loop Free	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Periodic Updates	Periodic &when needed	Periodic	Periodic	Periodic	Periodic & triggered	Differed by zone level	Periodic	Periodic	Periodic on associativity	No	Periodic	Varying Over Scope
Distributed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Critical Nodes	No	No	No	Cluster head	No	Yes	Yes	No	No	No	No	No
Routing Metric	Freshest & shortest path	Shortest Path	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path	Associativ ivity/route stability	Signal strength stability	Shortest path	Shortest Path
Network Size	Suitable	Not Suitable	Suitable	Not- Suitable	Not-Suitable	Suitable	Not- Suitable	Suitable	Suitable	Suitable	Not -Suitable	Suitable
Multiple Route Support	No	No	Yes	No	No	No	No	Yes	No	No	No	No
Multicast Capability	Yes	No	Yes	No	No	No	No	No	No	No	No	No
Security Support	No	No	No	No	No	No	No	No	No	No	No	No
WCC	O(2N)	O(N)	O(2N)	O(N)	O(N)	O(N/M)	O(N)	O(2N)	O(N+r)	O(N+r)	O(N)	O(N)
WCT	O(2D)	O(D)	O(2D)	O(1)	O(h)	O(D)	O(D)	O(2D)	O(D+c)	O(D+c)	O(D)	O(D)
Utilize Hello Messages	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No	No	No

N	Number of nodes in the route reply path
c	Diameter of the directed path
D	Diameter of the network
M	Number of zones, home region or clusters
h	Height of routing tree
WCC & WCT	Worst Case communication complexity & Worst time complexity

3. Issues in Internet of Things

The main issues relating to internet of things are as follows:

- *Addressing scheme:* For each device in the IoT, it is required that each device should have unique identification. The device can be detected in the network based on the unique ID. The data will be transferred based on the ID on each device.
- *Dynamic topology:* The devices in IoT are mobile in nature. Any device can join and leave the network at any time. So, the network keeps on changing all the time. Therefore, routing protocol should take in consideration the dynamic nature of the network.
- *False route:* is a way in which the data transmission follows an incorrect route. This can lead to looping in the network and the data will not be received by the correct destination.
- *Heterogeneous network:* The IoT is a vast network which contains various types of networks. Even if the devices in the network are varied in nature, they should be able to communicate with each other.
- *Inability to connect the device to internet:* even if the nodes are connected to each other sometimes these nodes are not connected to the internet which pose a problem while transmitting data.
- *Flooding:* It is a denial of service attack that floods the network. This leads to network congestion and increases the network traffic.
- *Node authentication:* the malicious node in the network should be rejected, if found to avoid loss of data. The authentication method should be able to authenticate the node for proper transmission of data.
- *Energy consumption:* As the IoT involves independent nodes in the network, self-powered and self-healing. Therefore energy consumption by each node should be taken care.
- *Fault tolerant:* if there is any fault in the link layer, there should be mechanism to resolve this issue. There should be multi paths in the network.
- *Scalability:* the IoT involves billions of devices connected to the network. The network should be scalable to handle many and various types of devices.[10, 11]

4. Problem Statement

As mentioned in section 3, there are different issues that slow down the communication process in internet of things. With heterogeneous network means different devices that have different capacity, geographical location, speed, and energy consumption. There is no unique identification for each object in the environment. Mostly devices in the IoT are low powered devices and have less computation capability. The energy consumption plays an important for the transmission of data in the network. In this paper, we propose a routing that allows different devices with limited resources and energy to connect to one another. The SDN Controller will provide a more secure network by denying access of the selfish node into the network.

5. Proposed Work

5.1 Assumptions

- The device registers with the SDN Controller
- The heterogeneous devices have different energy values
- A Centralized Controller monitors the overall traffic network

5.2 Algorithm

- *Step 1:* The nodes will register with the Controller. The Controller will assign a unique identifier for each node in the network.
- *Step 2:* The Controller will monitor the entire network

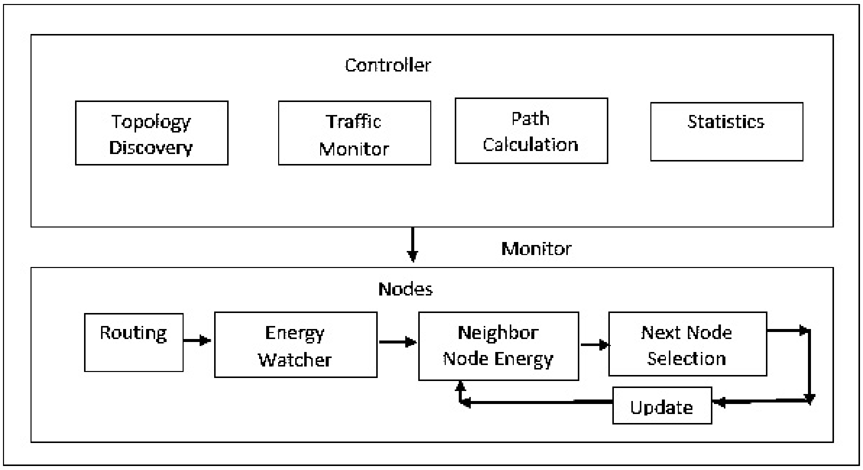

Fig. 2. SDN Architecture Integration with the Internet of Things.

- *Step 3:* The Source node finds information of neighbour node
- *Step 4:* Calculate the residual energy of the neighbour node
- *Step 5:* The source node will transmit the packet based on the energy value of the node. If the energy value of the node is below a threshold value, the packet is transmitted else select the other neighbour node.
- *Step 6:* The Controller will block the selfish node in the network and will not be allow to enter the network again.

5.3 Algorithm description

SDN is a software defined network that offers various services which makes the network more flexible and efficient. The devices in the network do not communicate directly but through a node called SDN controller that help to provide the forwarding decision. The Open Flow is a protocol that establishes a communication between SDN controller and the network devices. The forwarding rules can be changed dynamically depending on the nature of the network. The controller can update, delete flow entries depending on the forwarding rules. It provides a secure network since it establish connection between the end to end devices. It has a global view of the entire network based on the information received by the Open flow protocol. In addition, it also perform other network services like network discovery, security, routing, bandwidth management, traffic control, energy consumption, policy management, access control and topology configuration.

SDN separate the data plane from the control plane whereby allowing devices to just forward the packet. The SDN will control the behaviour of the network. It can also simplify the configuration of the network as well as maintaining the resources. This functionality of the SDN can be integrated with IoT to enhance the performance of the overall network. The dynamic nature of the IoT device can lead to frequent change in configuration. However by decoupling the data layer from control layer can help the network to adapt to frequent changes in the network.[13]

Each node will have the following attributes:

i. Source ID is the IP address of the source device.
ii. Destination ID is the IP address of the destination device.
iii. Residual energy of the device.
iv. Selfish list is the list of the selfish node in the network

The Controller will be having a table which consist of:

i. The IP address: indicates the IP address of the IoT device
ii. The Blocked List: list all the nodes which are selfish node in the network that has been blocked.

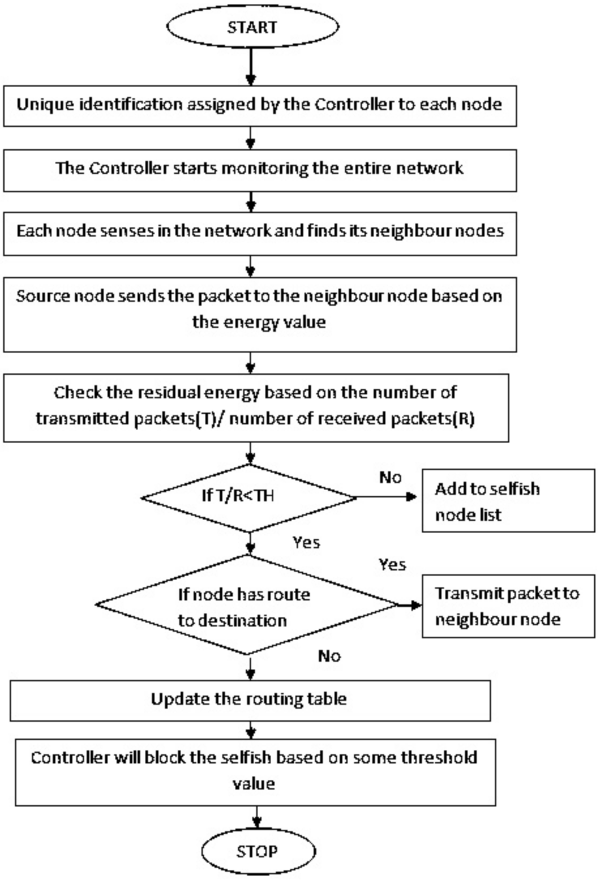
START
Unique identification assigned by the Controller to each node
The Controller starts monitoring the entire network
Each node senses in the network and finds its neighbour nodes
Source node sends the packet to the neighbour node based on the energy value
Check the residual energy based on the number of transmitted packets(T)/ number of received packets(R)
If T/R<TH
No
Add to selfish node list
Yes
Yes
If node has route to destination
Transmit packet to neighbour node
No
Update the routing table
Controller will block the selfish based on some threshold value
STOP

Fig. 3. Flowchart of the Overall Proposed System.

Each node that wants to join the network has to register with the SDN controller. A explicit and unique identification will be given to each node. Some node may not have the correct energy value and may behave as a selfish node. The controller has an overview of the whole network and keeps on monitoring the nodes. The selfish node can be easily detected by the Controller. If the device is below some threshold value, then the node is treated as the selfish node and will not have access to the network. If the new node wants to access the network, the controller will checks its IP address. If the node is in the blocked node list, the node will be blocked and deny access to the network.

A minimum energy level will be defined for the node in such a way that until and unless the node has a minimum energy then only it can transmit the packet else it cannot transmit any packet.

Te	Transmitted energy for each packet
Re	Received energy for each packet
Ecom	Energy consumed for transmission and reception of the packet
W	Size of the data packet
d	Distance between the two nodes
do	Threshold distance
Esd	Amplification Energy for short distance
Eld	Amplification Energy for long distance

Table 2. Simulation table.

Simulation Parameters	Values
Simulator	N-2.35
Number of nodes	50
Simulation time	3500
Energy model	Radio
MAC protocol	IEEE 802.11
Area	920*800
Initial Energy value	10 J
Initial Trust value	5
Packet size	512

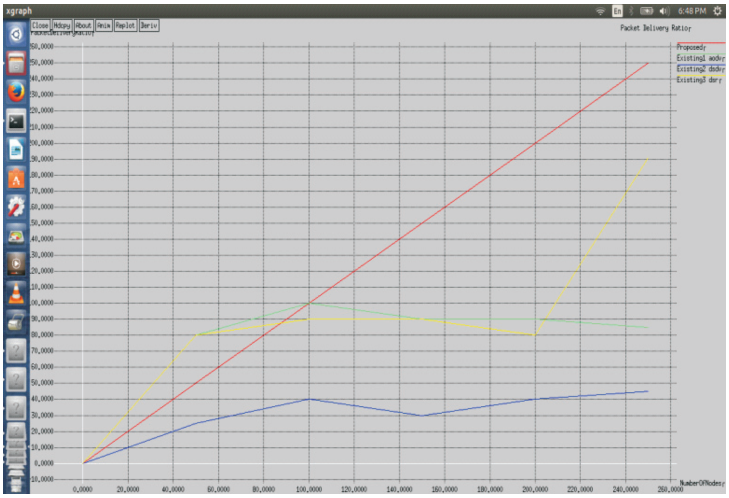

Fig. 4. Packet Delivery Ratio.

Threshold distance, do $= \sqrt{\frac{\text{Esd}}{\text{Eld}}}$.
Transmitting Energy,

- For short distance

$$\text{Te} = \text{W}^*\text{Ecom} + \text{Esd}^*d^2, \quad d \leq do$$

- For long distance

$$\text{Te} = \text{W}^*\text{Ecom} + \text{Esd}^*d^4, \quad d \leq do$$

Receiving Energy for each packet,

$$\text{Re} = \text{Ecom}^*\text{W}$$

Current energy of the node,

$$\text{Ecurr} = \text{Te} + \text{Re}$$

Residual Energy of the node,

$$\text{Eres} = \text{Eint} - \text{Ecurr}^{12}$$

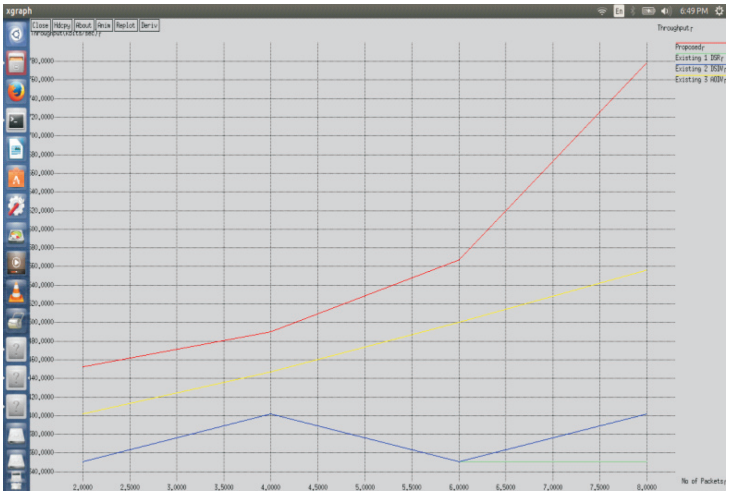

Fig. 5. Throughput.

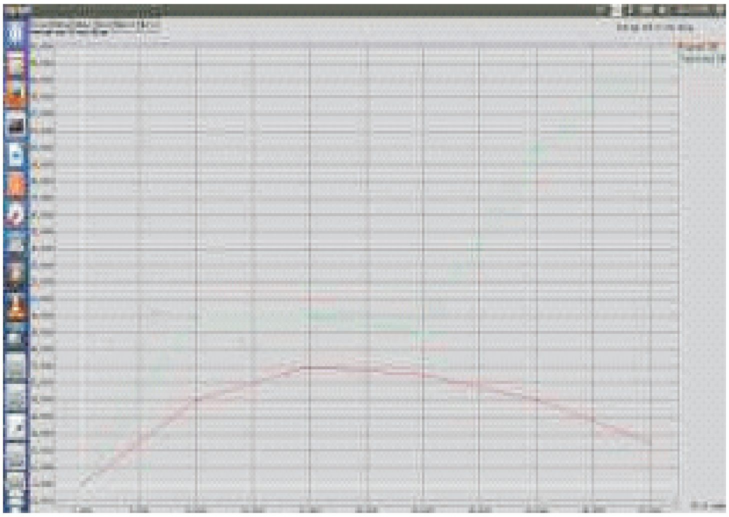

Fig. 6. Average End to End Delay.

6. Simulation

The proposed system is being simulated in NS-2 with version 2.35 using 50 nodes. Assuming the initial energy of 10 J and trust value of 5, the trust and energy value changes as routing progresses.

7. Analysis and Results

The proposed routing is compared for with other routing protocols AODV, DSR and DSDV routing protocol. Using the following parameters metrics

- Throughput: is the number of data rate that is how much a node can send a packet across the network. Throughput=received packet *8/ data transmission time.

- Packet delivery ratio: it is number how much packet is send to the destination
- Average end to end delay: is the total time taken for each packet to reach the destination.

8. Conclusions

In this paper, the routing using SDN Controller is compared with other routing protocols AODV, DSR and DSDV using the different parameters. The results shows that the proposed routing outperforms the other traditional routing protocols in terms of packet delivery ratio, average end to end delay and as well as throughput. Hence, using this proposed routing the overall performance of the network improves.

References

[1] Chris Lu, Overview of Security and Privacy Issues in the Internet of Things.

[2] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, Internet of Things (IoT): A vision, Architectural Elements, and Future Directions, *Future Generation Computer Systems*, vol. 29, pp. 1645–1660, (2013).

[3] Trang Tran Thi Thuy trang.tran@aalto.fi, Routing protocols in Internet of Things.

[4] Mohamed I. Gaber, Imbaby I. Mahmoud, Osama Seddik and Abdelhalim Zekry, Comparison of Routing Protocols in Wireless Sensor Networks for Monitoring Applications, *International Journal of Computer Applications (0975 – 8887)*, vol. 113, no. 12, March (2015).

[5] Adel.S.El ashheb, Performance Evaluation of AODV and DSDV Routing Protocol in Wireless Sensor Network Environment, *International Conference on Computer Networks and Communication Systems*, (CNCS 2012).

[6] Romana Rahman Ema, Ashrafi Akram, Md. Alam Hossain and Subrata Kumar Das, Performance Analysis of DSDV, AODV AND AOMDV Routing Protocols Based on Fixed and Mobility Network Model in Wireless Sensor Network, *Global Journal of Computer Science and Technology: E Network*, Web & Security, vol. 14, issue 6, Version 1.0, (2014).

[7] Padmini Misra, Routing Protocols for Ad Hoc Mobile Wireless Networks.

[8] Amit K. Kaushik, Performance Evaluation of Proactive and Reactive Routing Protocols in Wireless Sensor Networks, *International Journal of Computer Applications (0975 – 8887)*, vol. 110, no. 16, January (2015).

[9] Quan Le and Thomaz Magedanz, RPL-based Multipath Routing Protocols for Internet of Things on Wireless Sensor Networks, *International Conference on Advanced Technologies for Communications (ATC'14)*, (2014).

[10] Elizabeth M. Royer and Chai-Keong Toh, A Review of Current Routing Protocols for AdHoc Mobile Wireless Networks, *IEEE Personal Communications*, vol. 6, no. 2, pp. 46–55, April (1999).

[11] Dr. Neeraj Sharma and Simarjot Kaur, Overview of Various Routing Protocols in Wireless Sensor Networks, *Journal of Network Communications and Emerging Technologies (JNCET)*, vol. 2, issue 2, June (2015).

[12] Harsha Mishra, Vaibhav Kumar and Sini Shibu, Cluster Based Energy Efficient Routing Protocol for Wireless Sensor Network, *Engineering Universe for Scientific Research and Management*, vol. 7, issue 1, January (2015).

[13] Hai Huang, Jiping Zhu and Lei Zhang, An SDN_Based Management Framework for IoT Devices, ISSC 2014/CIICT 2014, Limerick, June 26–27.