2014 3rd International Conference on Eco-friendly Computing and Communication Systems

Resource optimization using Software Defined Networking For Smart Grid Wireless Sensor Network

Ruby Sayyed*, Sudeshna Kundu†, Chirag Warty‡ and Shikha Nema§
Department of Electronics and Communication
Usha Mittal Institute of Technology, SNDT Women's University, Mumbai, India
Email: *rubysayyed@ymail.com, †rimak100@gmail.com, ‡chiragwarty@ieee.org, §shikhanema@gmail.com

***Abstract*—There has been a decade of extensive research on application specific wireless sensor networks (WSNs). The recent development in communication network technologies makes it practical to realize a new WSN paradigm or controlling the control plane with the new group of by software defined networking (SDN) based on OpenFlow. The OpenFlow technology which is known for standardization and compatibility network Virtualization has brought a lot of innovative solutions in the field of research. In WSNs, sensor node are complex, highly dense and hence difficult to move. Network topology fast changes with time by using routing protocol, network topology, load balancing, power optimization, security and other factors. In this paper, the concept of SDN in WNS is introduced where OpenFlow is the controller part of network.**

Keywords: *Wireless sensor network, Software defined networking, OpenFlow, Smart grids, Routing protocols, Load balancing, Power optimization*

I. Introduction

With the Expansion of wireless communications systems , electronics and sensing technology, wireless sensor network (WSN) has attracted widespread attention [1]. WSNs are collected by the sensor with the functions of sensing, data processing, and short-distance wireless communication. In military defence, disaster relief, environmental monitoring, biological and commercial applications, and other fields have broad application prospects [2].

In traditional WSN generally adapts flat structure (i.e., single layer planer structure). A large number of sensor nodes with the same hardware structure, the sensing, processing, and communicating capabilities are deployed in the monitoring area, and transmit and forward information gathered by the other sensor nodes to sink node using the form of multi-hop under the help of other nodes within a wireless sensor network. And then wireless sensor network is connected with other types of networks by sink node, finally the user can remotely access, queries and manage the wireless sensor network. In flat wireless sensor network, the larger network size is, the more data lost in the communication path, and leading to worse network performance. At the same time, the large flat wireless sensor network also leads to intermediate nodes for forwarding data more energy consumption and energy heterogeneous problems arise.

In a wireless sensor network, routing protocol is one of key technologies and is presently one of the popular research problems. In multiple hops network, the data packet cannot be sent by the source node to the destination node directly and it has only relied on the help of intermediate nodes to forward grouped data. In the network intermediate nodes (including source node) must correctly determine which neighbouring node to send the received data packets and to find the shortest path to enable it to reach the destination.

The traditional characteristics of the wireless network does not exist in WSN. The architecture, addressing the method, the communication mode, and routing structures is different from the traditional network. Sensor networks have more nodes compared to other traditional network. There is no energy supplement but also energy is constrained in a WSN node. To improve the network's lifetime, routing protocol should get involved for to reduce energy consumption and load balancing. The existing routing protocols for wireless sensor networks have the following characteristics based on similarities and dissimilarities between WSN and other traditional networks:

Restricated Energy: The energy consumption is one of the challenges of wireless sensor network since a WSN nodes are numerous with weak mobility and irregularity in energy supply.

Local Topology Data : The big challenge for WSN is to save energy and ensuring efficient routing mechanism since the energy is limited.

High Topology Changes: Since sensor networks have more nodes, it is very difficult to move but its network topology showed a strong non-stationary, which requested that its high routing protocol must be able to adapt to the topology changes.

Particular Application: There are a wide variety of applications in WSN Environment, so there is no routing mechanism suitable for all applications, different applications adopt different systems.

Large Data Redundancy: Due to the random distribution of nodes in the existing WSN, there is no special logo on node, data redundancy information is great as multiple nodes collect the same data.

Due to a large number of sensor nodes and high density, sensor node energy, computing power, and storage capacity are limited. Hence, a new concept is introduced in Smart grid WSNs by SDN controller (Open Flow), where the whole architecture is controlled by "controller" part of the SDN.

978-1-4799-7002-5/14 $31.00 © 2014 IEEE
DOI 10.1109/Eco-friendly.2014.48

The content of the paper is as follows, the proposed system model is described in Section II, then in section III detailed description on Software Defined Networking is discussed, in section IV architecture of OpenFlow based on SDN is described in detail, in next section the comparison on WSN based on SDN with traditional routing protocol is done in brief.

II. System Model

The system model consists of one sensor control server and a set of software defined sensor nodes. To deploy a new sensing tasks, the sensor control server shall reprogram some sensor nodes by distributing a corresponding program to them for the task. Only the reprogrammed sensor nodes are able to sense the related targets within its coverage area.

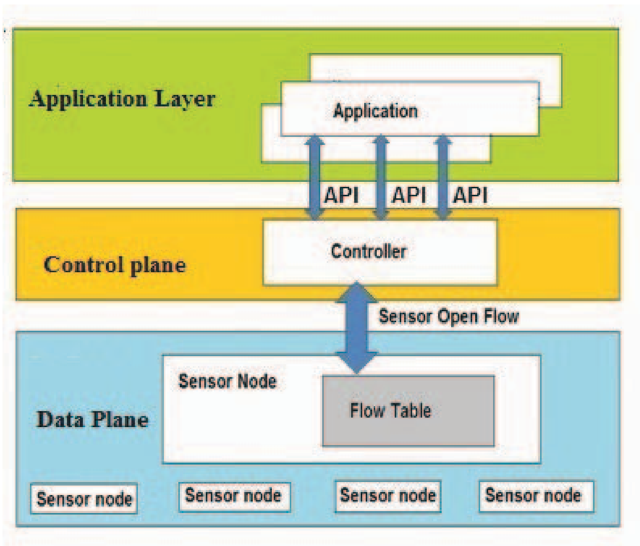

Fig. 1. Software-defined wireless sensor networks

In this paper, the first move is to tackle the above mentioned problems, using a radical, yet retired and peer well suited, approach. Software-Defined WSN (SD-WSN) is proposed. An architecture featuring a clear separation between a data and a control plane, and Sensor Open Flow (SOF), the core component of SD-WSN as a standard communication protocol between the two planes. The data plane consists of sensors performing flow-based packet forwarding, and the control plane consists of one controller that centralizes all the network intelligence, performing network control such as routing and QoS control. This architecture is delineate in Fig. 1. The whole idea is to make the underlying network (i.e., data plane) programmable by manipulating a user-customizable flow table on each sensor via SOF. The proposal is underpinned by the recently emerged software-defined networking (SDN) paradigm and OpenFlow [3], proposed for enterprise and carrier networks.

However, it is worth in exploring to introduce the fundamental idea of SDN into WSN and adjust it into a viable approach to solving WSN-inherent problems. The anticipation of SD-WSN to transform traditional WSN into networks are:

Versatile: Supporting multiple applications in a plug-and play manner; sensors are no longer application-dependent but application-customizable. This is achieved by (i) the programmable data plane which supports virtually all sorts of packet forwarding rules, and (ii) the control plane which decouples upper applications from physical devices (i.e., sensors) and provides a global, unified view of the underlying network to the applications.

Flexible: Easy to enforce policy changes throughout the entire network, which used to be a tedious task and is prone to inflexibility. This is achieved by the centralized and extremely granular network control in SD-WSN, where the granularity is supplied with the fully user-customizable flow tables.

Due to, high density, sensor node energy, computing power, greater sensor nodes and storage capacity are limited in WSN. so adoption of a new technology network topology changes frequently and has the self-organizing ability. When choosing wireless sensor network routing protocol there is a need to take into account the node energy, the communication load balancing, routing protocol fault tolerance, routing protocol security mechanisms, and so on.

III. Software-Defined Networking

SDN is an emanate computer networking approach that allows network administrators to manage network services through the abstractions of low-level networking functionality. Such paradigm is realized by decoupling the control plane and data (forwarding) plane. By such means, the functionality of the network can be defined, or reconfigured, via a standard programming interface (e.g., OpenFlow) according to the transmission requirement after it has been deployed. For example, via OpenFlow [3], the forwarding rules are defined for different flows and the corresponding actions (e.g., drop, forward, modify, etc.) will be taken once a packet match a rule. SDNs, with the potential to dramatically simplify network management and enable innovation through network programmability, propose the concept of Sensor Openflow and thus SDN technique provide a promising solution to network management in WSNs.

IV. Architecture of OpenFlow Based on SDN

Network forward separation proposed by proprietary equipment deployment of high-level strategy under the guidance of senior policy data forwarding can be done. In SDN two part open flow switch and controller open flow switch forward packets according to the flow table. Forwarding plane controller achieves the control function through the network view. The control logic represents the control plane [4].

In Smart grid wireless sensor network the flow of SDN is controlled. The contol funtion of the traditional distribution network equipment will migrate to the controlled computer device. The Application, control and infrastructure layer open programmable software pattern realize the automation of network control function. Smart grid wireless sensor network model consists of three basic roles: master node, center node, normal node.The master node act as the open flow controller of the network structure (programmable control unit of the central executive) according to the control unit (including topology, transmission capacity, and routing restrictions) will decide how to achieve synergy and interaction between nodes for themselves. Open Flow Switch(center nodes) function of center node is similar to the OpenFlow switch. It is responsible for matching and forwarding data stream in the wireless sensor network. The responsibility of normal node is only to receive data flow.

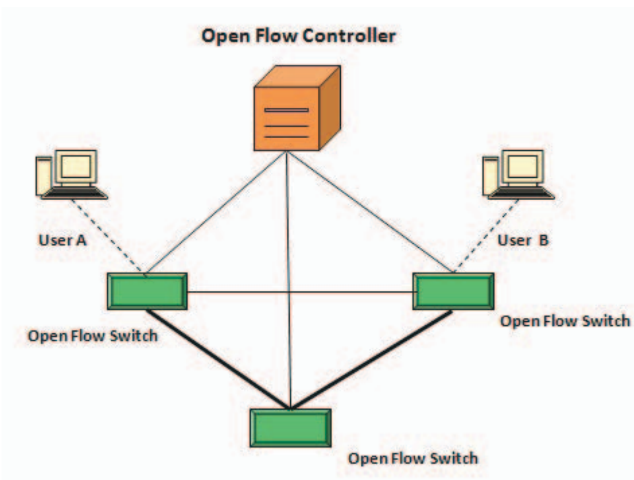

Fig. 2. Open flow based WSNs toplology

In Fig. 2. controller (master node) sends a feature-reguest message as soon as TCP hand shake is done. The connected Open Flow switches (center node) reports with a feature-reply message. The feature-reply message gives information to the controller about the switch capabilites, port deatails and action capabilites. In second step, the inter switches links discovery happens using LLDP [5] link layer distribution protocol frames that are sent on all conected ports of the swtiches between different Open Flow switches. All the LLDP [5] frames are actually made by the controller and sent by using a packet-out event from the contoller with an action to send on all or up state ports. Once the controller has all packet with it will have a view of the full topology.

A. Master Node/Controller

In SDN controller is the master node or core node of the NOS network to realize control logic function. NOX is central controlled execution unit of the Open Flow network in Fig. 3.

In Smart grids WSN, based on the OpenFlow/SDN, NOX by maintaining the basic information of the network view to maintain the entire network. The Network unit provides service. The application runs in the top of NOX by calling the global data network view to operate a centre node in the entire network in the software defined network

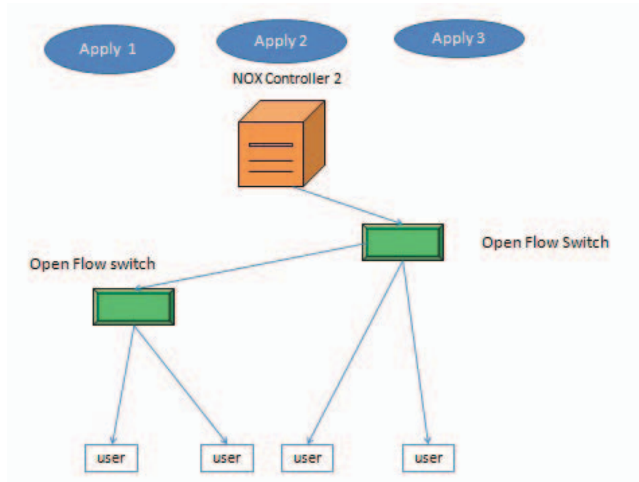

Fig. 3. NOX-based OpenFlow network.

Controllers are directly deployed in real network and solve the problem of multiple controller to Open Flow switch control sharing at the same time as in Fig. 4. makes hardware

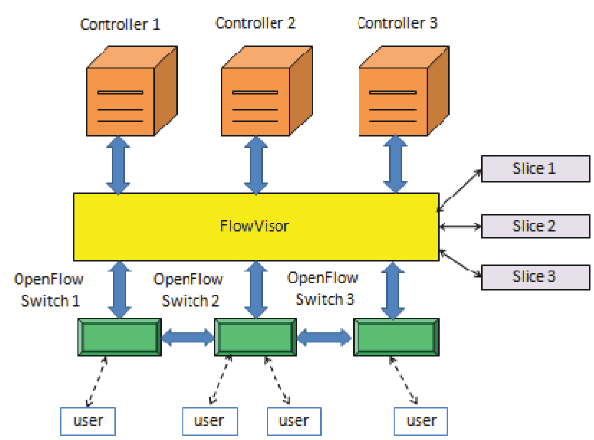

Fig. 4. FlowVisor based OpenFlow virtualization.

forwarding plane able to be shared by multiple controller can manage and switch at the same time and network administrator can control network in parallel. So that traffic engineering is achieved in open flow Virtualization network traffic can run on a separate slice mode.

B. Center Node/OpenFlow Switch

OpenFlow switch is responsible for data forwarding function. Main technical details are made up of three parts: flow table, secure channel, and OpenFlow protocol Fig. 5. Each OpenFlow switch processing unit consists of flow table, and each flow table is made up of many flow table entries.Flow

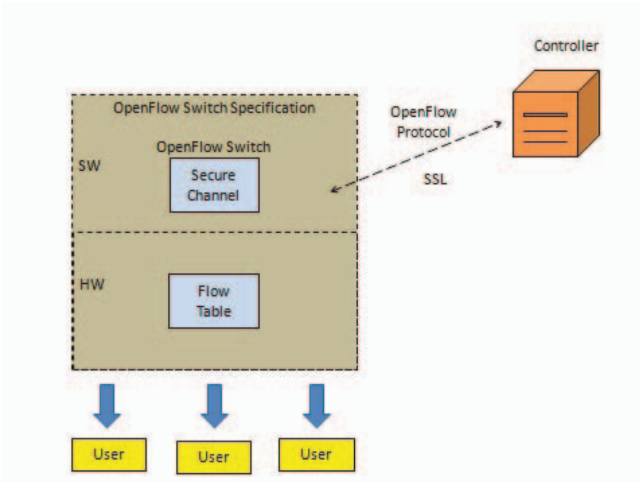

Fig. 5. OpenFlow infrastructure

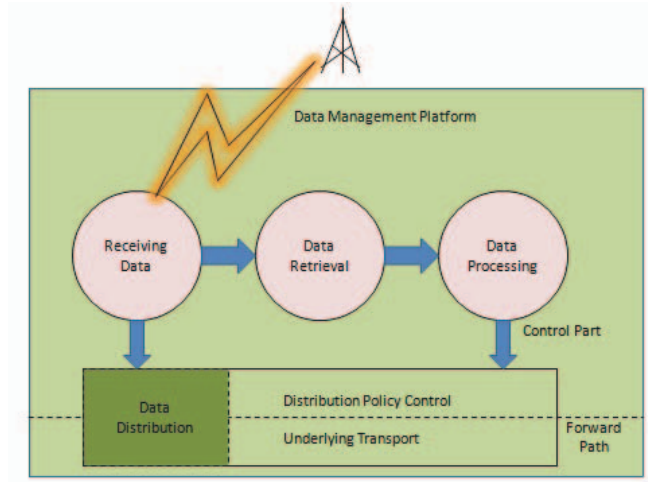

Fig. 6. WSN based on OpenFlow network

table entry represents the forwarding rules. In traffic engineering to enhance the efficiency of the query traffic , in flow table many multiple stages for flow table and pipeline mode.Flow table item is mainly composed of match fields,counters and instructions. The structure of matching field contains a lot of matchs, as the link layer,network layer and transport layer identifies. The counter is used for statistical basic data stream. Action represents the data packets which have been matched with the stream table entry and should perform the next step.

Secure channel is an interface that can connect OpenFlow switches to controllers. Through this interface configuring and management of OpenFlow switches can be obtained by the format specified of OpenFlow protocol. Apart from matching flow table item, center node needs to identify various existing WSN routing protocols, by reserved interface it is convinient for extensions in the future [6]

C. WSN Based on OpenFlow Network Structure

In Fig. 6., this network architecture central node is controlled by the master node ,the particular forwarding strategy entirely depends upon the master node, the whole message link is completely controllable, when nodes are in abnormal condition such as fault conditions, energy depletion the master node can adjust strategy or change the forwarding path.

The whole core framework depend upon information dissemination strategy. The master node make a connection to the transmission path and passed information according to the QoS of the information. The master node through the secure channel among the center node and master node can generate flow table.

When the center node first received the information forwarding requests, the center node matches the flow table information and will feed the node information back to the master node.

After it receives the feedback information, the master node begins to construct an optimal forwarding policy based on the information of QoS and the network topology maintained by the center node.

When the master node has chosen a path, the center node will be informed through the flow table to be added to it. When the information arrives at the center node, the message can be forwarded according to the strategy that has been built. Because the forwarding strategy is the optimal path chosen by the QoS, node status, and the network topology, the message forwarding efficiency will be very high.

When the information is sent over and the next flow of information arrives, the center node will check the flow table at first. If the information can be matched with the last, it means the QoS, node status, and the network topology are consistent with the previous one. There is no need to construct a new forward path. If the flow table exists, a flow table entry cannot be forwarded, center node will feed the information back to the master node and request the construction of a new path.

Since every information forwarding has selected the optimal strategy and fully controllable, the stability and flexibility of the network much higher than traditional WSN routing protocol.

D. Center Node Deployed in WSN Network

Primary challenges of WSN is data aggration, load balancing, location tracking. WNS sensor nodes are tiny cannot be easily rechareged once they are deployed. Untill now many energy efficient routing algorithem or protocol have been proposed with techinigues like clustring, data aggregation and location tracking. The aim is to minimize parameter like tatal energy consumption, latency etc. by using Distance based energy Aware Routing (DEAR) algorithem [7].

The distance between two points by using cosine similarity to compare and calculate resemblance of two primary frequency plot after the calculate the distance between two points. frequency plot is the numerical expression of the relative position based on the CDN network [8]. It is a set of n-dimensional

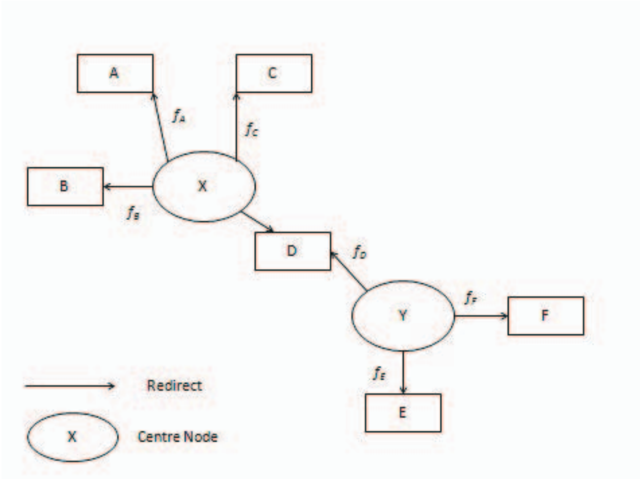

Fig. 7. The relative position to determine.

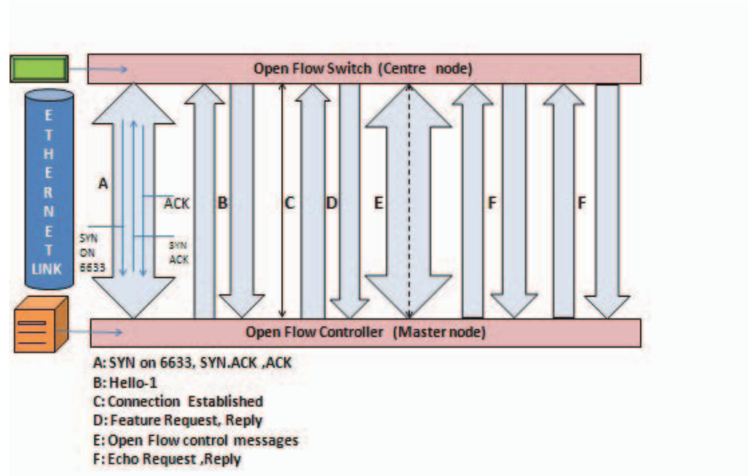

Fig. 8. connection between center node and master node

vector.It account the redirectioanl data/information in a fixed time interval from the CDN network.

By the cosine similarity formula, a, b are vectors, respectively, put into the formula; we obtained two primary frequency figures a and b are obtained as follows:

$$Cossim(a,b) = \frac{\sum i \epsilon I_a (u_{a,i} \, .u_{b,i} \,)}{\sqrt{\sum_i \epsilon I_a u_{a,i}^2} \cdot \sqrt{\sum_i \epsilon I_b u_{b,i}^2}} \quad (1)$$

From the above theory the rough distance between the nodes corresponding to primary frequency plot formula is obtained. Based on the division of Land Mark, for Z a Land Mark, the n-dimensional space of CAN can be divided into Z Parts which follow the physical distance.

In Fig. 7., X be the center node. In clusturing area center node represent physical center area. Center node can cover the areas by junior or senior frequency diagram, depends on the measurement system.

E. Connection Establishment between Center nodes and Master node

The connection between Open Flow controller(master node)and switches(center node)by sending sequence of packets, which are needed for successful connection and exchanging of packets. A simple event of connection establishment is shown in Fig. 8. The explanation of these connection are given in various steps:

Step A: When a Open Flow controller (master node) and Open Flow switch comes up, the connection initiates with a TCP three-way handshake procedure. The TCP port number used is 6633.

Step B: Once TCP connection over, the hello packet is a uniform packet in OpenFlow protocol. The hello packet has no content in it; Open Flow general header is the only content for hello packet, with "'Type value=0"'.

Step C: After the hello packet are exchanged, the connection established between controller and switch. Then it is checked with controller GUI (Graphical User Interface) or switch CLI(Command Line Interface, based upon vendor implementation.

Step D : Feature request, this the controller switch message that is sent by controller to determine the switch capabilities and all other particular charactertics item runing on Open Flow switch. The packet has no content, and a Open Flow general header is used for feature request, with "'Type Value=5"'. Feature reply. This is the controller switch message that is sent by the switch(center node) to the controller [9].

Step E: Once the controller or master node knows the center node (switch) capacity, all Open Flow protocol-particular action can start.

Step F: Echo request echo reply are uniform types of packets in Open Flow.These are used as keep alive message between the Open Flow controlle r(master node) and Open Flow switch (center node). Typically the Open Flow header is used for echo request ("'Type value = 2"') and for echo reply ("'Type value = 3"'). The payload of echo request and echo reply can be changed according to the implementation by other vendors.

F. Open Flow protocol

In Fig. 9., it is a basic flow digram between an Open Flow (Switch)and Open Flow Controller (Server):

Various events are happend in connection established between Open Flow controller and Switch as described below:

Packet-In Event: This event explain the triggers and content of the packet-in event. The trigger would be form the switch for a packet-in event is generated when a packet is recived by an Open Flow switch and ther is no match in the flow table or the packet matches one of the entries with the action of sending output to the controller. Once the paket-in condition is triggered on the center node switch , the packet-in event is constructed and send to the controller.packet-in header contain the following:

Buffer ID,Packet length.

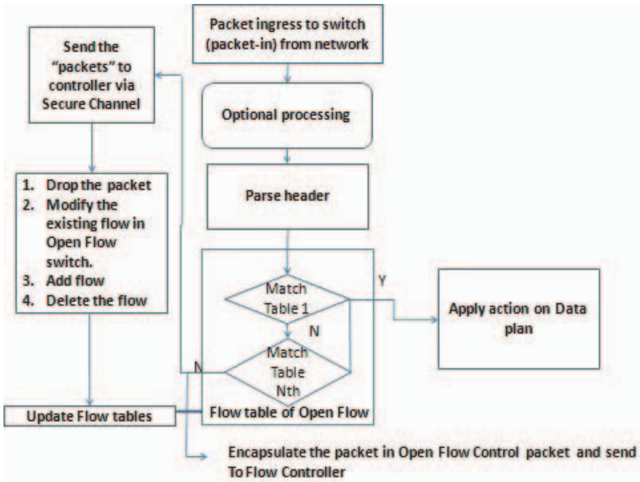

Fig. 9. Flow digram of Open Flow protocol

Input port: Reason: 0; No match, 1; Flow table mention to send packet to controller explicitly.

Data frame: The actual packet the Open switch received.

Packet-Out Event: The packet is sent from the controller to the switch.The details are in packet-out type,encapsulated in Open Flow header. The deatails of Open Flow packet-out carreier are: *Buffer ID,Ingress port number*.

Action list(Added as action desriptor):Output action descriptor, VLAN PCP action descriptor, Strip VlAN tag action desriptor, Ethernet address action desriptor, IPv4 DSCP action desriptor, Ingress port number, TCP/UDP port action desriptor, Enquence action desriptor, Vendor action desriptor.

Other Events are like: Port Status message, set configuration, get configuration request and reply, flow modification, flow removed and port modify event [9].

V. Conclusion

While comparing the difference of number of death nodes between LEACH [10], LEACHM [11], and DEEC [12] routing protocol and WSN structure based on the technology of SDN ignoring the influence of wireless channel interference it's been found that the death node appeared when LEACH, LEACHM, and DEEC protocol execution are 1000-1300 times.When the system runs 2500 times, all the nodes are dead while in case of the new structure all the node died when the system ran 3000 times. So compared with traditional routing protocol, WSN based structure is more stable.

Similarly changes in energy consumption, the new structure is relatively more stable and remains on a lower power consumption level. When the network topology changes, some nodes consumes high instantaneous energy but comparing the new structure with traditional routing protocol though in new structure some nodes have high instantaneous energy consumption, the life of the network is longer that traditional routing protocols. In the process of work, LEACH and LEACHM protocol need to select the clusters heads several times due to the limitations of the protocol they cannot guarantee the efficiency of the network and the nodes.Thus, are not efficient in controlling node energy, load balancing, and topology changes.

In this paper, using Smart Grid WSN, all sensing nodes are connected through one master node which is the controller(OpenFlow). Controller is relatively in fixed position and it can flexibly choose routing protocol according to the change of network topology. Thus, minimizes network complexity, power optimization in sensor nodes, speed and other factors.

Acknowledgment

We would like to thank Dr. Sanjay Pawar for being a constant source of inspiration to us. We are also thankful to all the faculty and staff of UMIT, Mumbai, India for providing the support and facilities to carry out our research and project work without which this wouldnt have been possible.

References

[1] Zhi-jie Han and Wanli Ren,"A Novel Wireless Sensor Networks Structure Based on the SDN", *International Journal of Distributed Sensor Networks*, Vol no.2014, PP. 1-7, 2014

[2] F. Zhao and L. Guibas," Wireless Sensor Networks: An Information Processing Approach," *Morgan Kaufmann, Boston, Mass, USA*, 1st edition, 2004.

[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, No. 2, PP. 69-74, 2008.

[4] M. O. Pervaiz, M. Cardei, and M. Wu, "Routing security in ad hoc wireless networks," in *Network Security,Springer, NewYork, NY,USA*, PP. 117-142, 2010

[5] Vahida Z. Attar, Piyush chandwadkar, "Network Discovery Protocol LLDP and LLDP-MED, in *2010 International Journal of Computer Applications*" Vol.1, No.9 PP. 0975 8887, 2010

[6] S. K. Singh, M. Singh, and D. Singh, "Routing protocols in wireless sensor networks - a survey", *International Journal of Computer Science & Engineering Survey,* vol. 1, No. 2, PP. 63-83, 2010

[7] Jin Wang, Jeong-Uk Kim, Lei Shu, Yu Niu and Sungyoung Lee," A Distance-Based Energy Aware Routing Algorithm for Wireless Sensor Networks," *PMC,Sensors (Basel),*Vol 10, No.10, PP. 9493-9511, 2010

[8] Z.J. Han, L.S. Huang, R.-C. Wang, L.J. Sun, and M. Sheng,"Distance aware route algorithm for cloud computing based on CAN," *Journal on Communications,* vol. 32,No. 7, PP.29-39,2011

[9] Vishal Shukla, "Introduction to Software Defined Networking, Open Flow and VxLAN" *CreateSpace Indepedent Publishing Platform,*, North Charleston, 2013.

[10] O. Younis, S. Fahmy, " HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks", *IEEE Trans. Mobile Comput.*, Vol.3,No.4, PP. 366-379, 2004

[11] Sapna Choudhary, Sandeep Sharma, "A Survey of LEACH Protocol and its Modified Versions in Wireless Sensor Network," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.4, No.1, PP. 850-853, January 2014.

[12] K. Latif, M. Jaffar, N. Javaid, M. N. Saqib, U. Qasim and Z. A. Khan. "Performance Analysis of Hierarchical Routing Protocols in Wireless Sensor Networks" NGWMN with *7th IEEE International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2012)*, Victoria, Canada, 2012.