International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 147 –155

Improve Quality of Service Using Cluster Head Selection in Software Defined Wireless Sensor Network

Munaf Kapdi, Umesh Raut

School of Computer Engineering & Technology, Dr.Vishwanath Karad MIT World Peace University,
Pune, Maharashtra, India
0munafkapdi@gmail.com and umesh.raut@mitwpu.edu.in

Abstract

Today, the commercial wireless sensor network (WSN) are increasingly evolving a wide range of applications with specific specifications, and offering the quality of service for this kind of communication system is unavoidable. The issues of poor adaptability and complexity in implementing the qquality based implementation and management within conventional system architecture are difficult to address. The wireless nature of contact makes the nodes vulnerable to attacks of a number of types, such as whole black attacks, wormhole attacks, denial of service attacks. Now current effort, we aim to improve the quality. We have proposed two Cluster Head (CH) selection algorithm based on the available trust and energy avoids the energy hole phenomenon and reduces the workload of a single cluster head. The unified routing algorithm builds two heterogeneous node forwarding paths that satisfy the requirements for different data rates. Local network maintenance decreases the number of network access notifications. The simulation results show that the quality support for data can provide different requirements, balance the network energy consumption and extend the lifetime of the network.

Keywords— *SDN, WSN, quality, Cluster Head, heterogeneous*

1. INTRODUCTION

Networking is key part today as the whole world is only connected to each other with the help of it, but not every one is meant to access or modify that data, as so in an industry not all employees are meant to access all the data, rather then separately securing each and every single employees, permission can be assigned at once for the group of users who work on same profile and need the access of similar and only that data or resources can be made available with the help of SDN. The WSN on other hand is an sensor network at the end where the sensors sense the data and transmit it to the sink node by selecting the path between nodes nearby. Consisting of both this technology is SDNWISE where the sensors sense the data transmit to the sink node and the sink node then proceeds the data to the SDN controller where it can be processed. To do the work of transmitting the data from the sensor node to the sink node is done by the Cluster Head. All the data is sent to the Cluster head by the sensor nodes and then it finds the best path by selecting the neighbouring nodes and forwarding the data to the sink node.

In our simulation we will try to use two cluster heads instead of one that is traditionally being used so that if one of the cluster head fails, the work of the network wont stop there wont be any unnecessary packet drop, which will indirectly improve the quality of the network, we will pro long the network lifetime and try to resolve the bottleneck issue that occurs at the sink node usually due to degradation of batter as only one node is present to handle all the load.

Cluster head will be selected based on the fitness property of the Genetic Algorithm, where the node with highest energy will be assigned the role of Cluster Head and the one with the second highest enery will be assigned the role of second Cluster head.

ISSN: 2233-7857 IJFGCN

We will have real life example simulation in the case where the Cluster head fails due to the drainage of the batter, due to any kind of failure or a flooding attack where an user floods the system by transmitting hundreds of thousands of data simultaneously on the cluster head. In all of this conditions we will change the path of the data transmission from the normal cluster head to the other cluster head.

The path will be selected using the BTC algorithm which will find the nearest node in the direction of sink node taking less energy and cost for traversal of the data. The data traversal will then be done by the DATA AGGREGATION protocol which will check for the presence of data or not if non zero will transmit the data till being zero.

2. RELATED WORK

Wenbo Zhang, Yue liu1, Guangjie Han, (member, ieee), Yongxin Feng, and Yuntao Zhao [1], in industrial wireless sensor networks, an energy-effificient quality-of-service (QoS) routing algorithm is very important to ensure that the key sensing data can be forwarded in a reliable path and solve the energy balance problem. In this paper, we classify the industrial sensing data into three data types and set their priority. Furthermore, we give the reliability parameters and timeliness parameters, and we propose and establish the candidate forwarding node set in order to balance the energy consumption. Subsequently, an energy-effificient and QoS aware routing algorithm is designed, and in this routing algorithm, different kinds of data can be forwarded with different strategies. Furthermore, the most important industrial sensing data are guaranteed to be transmitted to the sink node reliably and timely and common data can be transmitted effec tively, too. All these data will be forwarded to the optimal relay node under the circumstance of that the data requirements of real time and reliability are satisfified. The simulation results show that the high timeliness event data can be transmitted real time and reliability than the other type of data. And our proposed routing algorithm is effective compared with the similar algorithms

Jeremy A. Stone, Neetesh Saxena, and Huseyin Dogan [2] to reduce the amount of information exchanged between sensor nodes and the SDN network controller, to make sensor nodes programmable as fifinite state machines so enabling them to run operations that cannot be supported by state less solutions.introduced.

Ali Abdul-hussian Hassan, WahidahMd Shah, Ali Mohamed Husien, Mohammed Saad Talib,Ali Abdul-Jabbar Mohammed,MohdFairuz Iskandar [3] Clustering approach in wireless sensor network is very important, the structure of cluster and how to improve it is a fifirst challenge that faced the developers, because of it represent as a base for design the cluster-based routing protocol.

Zhaopeng Jia Xiang Cui Qixu Liu Xiaoxi Wang Chaoge Liu [4] With the wide application of wireless sensor networks (WSNs), secure data sharing in networks is becoming a hot research topic and attracting more and more attention. A huge challenge is securely transmitting the data from the source node to the sink node.

Rajan Patel Anal Patel, Nimisha Patel [5] this assessment is Based on various methods used to identify writers of the wormhole attack, an attack line was placed forward for the detection and hindrance of wormhole attacks. A projected methodology for defensive against wormhole attack based mainly on the Hash-based Compression Function (HCF) which is really mistreatment of any secure hash operates to encrypt a hash field for the RREQ packet and the expected methodology appearance as opposed to other future solutions of literature.

Dhruva Patel et. al. [6] system defines how not the same security layers are unfair by a number of security threats. Due to its softness and self-routing natural surroundings, MANET faces many risks and can carry out various attacks on the pillars in the network. There There are a number of attacks, and each attack has its own effect on different layers, just as some networks can only affect the layer, while others may target other layers depending on how they respond. A wormhole attack is actually an intrusion of a network layer that can completely interrupt the communication channel, and has been found to be a very serious threat in all attacks. The authors illustrate the wormhole attack in this paper, and discuss various existing detection and prevention techniques. In those techniques, wormhole attacks appear using AODV and DSR routing protocols and other routing protocols such as Torah, ZRP, wormhole should be used to detect attacks.

ISSN: 2233-7857 IJFGCN

Juhi Biswas et. al. [7] system present the AODV routing protocol has been modified to track and prevent real-world wormhole attacks, and this adapted AODV has been implemented with the wormhole threat detection and prevention strategy (WADP). The authentication function of the node acts to identify malicious nodes in the network and eradicate false positives. In contrast, the duplicate outcomes Show that the node does not simply delete authentication the false positives but also helps to create the actual location of the holes together, and there may be double verification to detect whole attacks. This algorithmic rule doesn't usage any singular hardware for police work wormhole attack.

Kapil Raghuwanshi let. al. [8] Take the initiative to fix or that a hole attack by responding that the existence of a hole is felt during the initial route setup process. This resolution is predicated on step sum total learning method i.e. hop sum total is employed as a constraint for characteristic ways containing hole tunnel. Step calculation analysis is employed to spot hateful nodes. Virtual reality of the projected effort is completed within the being there of hole attack in numerous node and traffic situations. The imitation results projected method shows superior show as PDR and turnout will increase but, “average end-to-end delay” additionally will increase. Within the analyzed state of affairs, it's found that the MAODV includes a superior presentation then AODV. Changed AODV is appropriate for finding and bar of hole attack. It advances the Packet delivery magnitude relation vulnerable state of affairs, with a borderline decrease in turnout and suitable increase in end-to-end delay.

System [9] Light wormhole attacks that are unsafe for packets when two or more malicious nodes are tuning into a relay structure. This type of attack will submit changes to selective routing, falsification, and packets. This paper, AN characteristics primarily created signature theme at the side of clusters is planned for shielding network from whole attack. The planned theme doesn't need Therefore, any credential distribution between nodes reduces overhead computing. During which the cluster head area unit was selected in such a way that they could not be malicious, a predominantly based design was employed. This theme works in three stages. Simulation results show improved performance through expected theme throughput, packet delivery ratio, and end-to-end latency.

According to [10] proposed The protocol is based on neighborhood overhearing and on a continuous review of the main and different tables ' details, and the intended protocol is found to be safe, and a few units of the attack area are tested. Attack to the wormhole is detected by overheard nodes. The results show that in terms of the packet delivery magnitude relationship, M-AODV has been improved and therefore the delay has been decreased yet, but the overhead quantity has been increased. M-AODV jointly increases network reliability and safety. The area unit has features such as overhear, immediate modification, native repair, and 2 routing tables when safety measures are taken. It’s assumed that the planned protocol could act like other secure strategies, like neighbor overhearing (NEVO) and Packet time period (PTT), that be necessary a number of these options yet and should be secure against certain attacks. Thus, in virtual reality, the planned protocol is shown to be protected alongside wormhole and blackhole attacks.

3. PROPOSED SYSTEM

In our system that we proposed here has three of its main plains, first where all the sensor nodes, normal nodes, sink node and the cluster head is present. In this plain the sensor node will sense the data find the nearest node to cluster head or the cluster head itself and transfer the data to it. Then the BTC algorithm will find the best path toward the sink node (the switch mentioned here are the sinks)

The sink node is the one point communication between both the upper and lower plains that is it will only communicate on both the side that is getting information form the sensor nodes and providing it to the controller.

The controller on the top plain will process the data according to its needs also it could just gather the data and analyse it for some betterment in the future.

ISSN: 2233-7857 IJFGCN

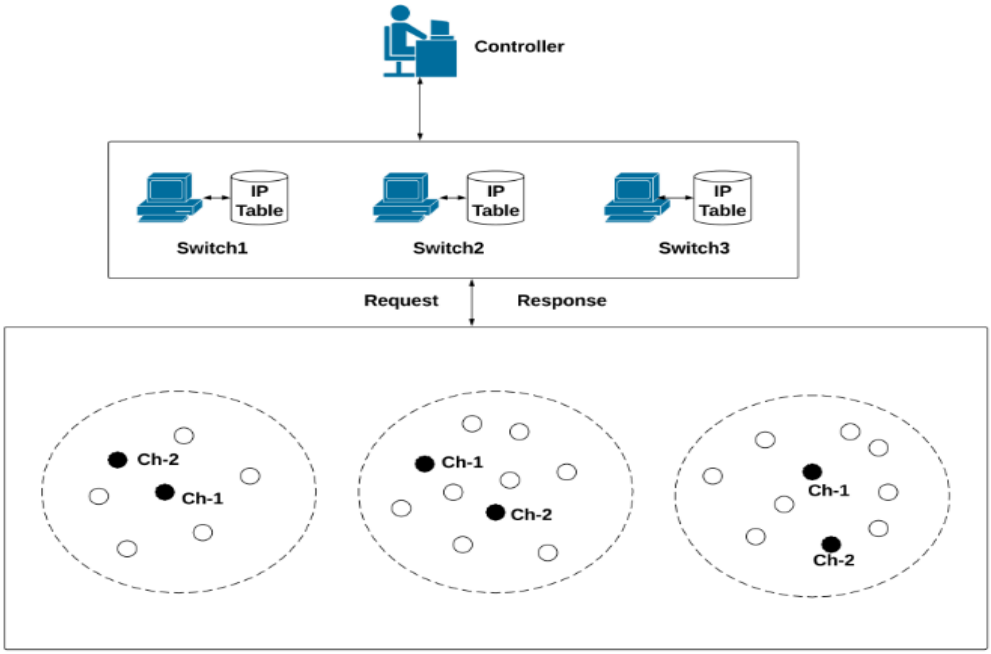

Figure 1 : Proposed system architecture

In this work we have carried out an algorithm which provides effective data communication through in a cluster based network in SDN. Basically AODV routing protocol is utilized as the fundamental network topology. A multi-layer method is used for detecting whether a node is participating in a decent communication or attack. The layered approach is introduced to decrease the capacity of dispensation on respective cluster heads. Due to safety point of view, this also decreases the risk of a cluster head should be hacked by attacker. The complete network is separated in clusters sets illustrated in figure 1. Sometimes clusters might be corresponded or separate. Every cluster contains a two cluster heads as well as number of cluster member nodes. Member nodes forward on the data only to the cluster head when any nodes want to send data to Cluster Head (CH). The CH is responsible for forward on the collective data to all its other cluster members. The CH is selected enthusiastically and preserves the routing information, only the major benefit this framework than other SDN approaches it works with two cluster heads. When CH1 having congestion at same time CH2 activates and perform similar task which eliminates packet loss issues and improve the quality. In other hand BTC also works for secure data transmission with shortest path find method which reduces the time.

Algorithm Design

1. Approach for Cluster Head (CH) Selection

Input: Cluster set with nodes.
Output: Ch selection with remaining sensor node.
Step 1: select all nodes as initial population.
Step 2: Select evaluation set
Step 3: Apply crossover on similar power nodes.
Step 4: Apply mutation on each sensor node.
Step 5: Apply fitness on all nodes power
Step 6: select best node using rout let wheel selection.
Step 7: Check GA evaluations
Step 8: Select final max energy node as CH node.

2. Construction of BTC for best node selection

Input: Primary source node *Sender_node,* Destination node *Dest_node,* Group of nearest nodes Neigh_node *[],* node id as *N_id,* node energy *N_eng;*
Output: From source to destination way based on the given algorithm.
Step 1: initially system select the *Sender_node* and *Dest_node* on dynamically
Step 2: select the packet or file f for info broadcast.

ISSN: 2233-7857 IJFGCN

Step 3: if (*file or data* ! =null)
Step 4: read each byte *bytes* form *file or data* when reach null
Step 5: send data, initialize *cost_filed_1, cost_filed_2, parent_filed_1, parent_fileld_2*
Step 6: while (nd[i] when reach NULL)
cost_filed_1=node[i]_eng
parent_filed_1= node[i]_id
cost_filed_2 =node[i+1].eng
parent_filed_2= node[i+1] _id
Step 7: if (*cost_filed_1> cost_filed_2*)
cost_filed_2=null
parent_filed_2=null
Else
parent_filed_1= parent_filed_2
cost_filed_1= cost_filed_2;
parent_filed_2=null
cost_filed_2=null
Step 8: end of while loop
Step 9: reiteration till when extent at the sink node

3. Data Aggregation Protocol

Input: existing received data list as TPQ, current received

packet list IP

Output : 1 if aggregation is possible else 0

Step 1 : for each (data into TPQ) using below formula

$$\text{Data[i]} = \sum_{k=0}^{n} \text{p[k]}$$

Step 2 : validate the similarity between Data[i] to IP[0]

Result {0,1} ← calcsim(Data[i] , IP[0])

Step 3 : end for

Step 4 : return Result

4. RESULTS AND DISCUSSION

We present an assessment of the proposed system in this section. After explaining our experimental setup, we quantitatively test the analysis for the various parameters used, such as drop rate(DR), throughput and packet distribution ratio(PDR). We are presenting your experiments in version 2 of NS2 Simulator. In. That demonstrated practical outcomes. The NS simulator runs TCL code, but for header input we use both TCL and C++ code. In our simulations we use the infrastructure based network environment for communication. Providing access to wireless networks that have never been used to pick a network. NS2 replication of WMN. TCL file show the simulation of all over architecture which proposed. For run . Using the NS2 simulator system, TCL also helps to store running connection information messages using the US1 communication pattern script. You can use the NS2 trace file.TR to evaluate the data. It supports vector and scalar data collection, encoding and display. The results folder of the project folder contains the us.tr file, which stores the simulation output information. Created on the us.tr file, we have created a database of 5 text files which contains reading of 5 ms each till 25 ms as our simulation time is 25 ms. After that, we read the text file in a program created for the trace in Netbeans IDE 8.2. We got readings of various events in Netbeans from which we have plotted the graph of various parameters such as Drop Rate(DR),Throughput and Packet Delivery Ratio(PDR).

ISSN: 2233-7857 IJFGCN

The simulation parameters has used which is described in below table

Parameter	Values
Simulator	NS-allinone 2.35
Simulation time	25 Seconds
Channel-Type	Wire-less Channel
Propagation-Model	2 Ray Ground
Standard	MAC/802.11
Simulation Size	1000 *1500
Max packet Length	1000
Ad hoc routing	AODV
Traffic	CBR

1. Drop Rate:

It is defined as the number of packet lost per number of packet sent. The minimum total value of drop rate statuses superior presentation of the protocol.

$$Drop\ Rate = \sum_{i=0}^{n}\left(\frac{packet\ received\ [i \ldots n]}{sent\ packet\ [i \ldots n]}\right)$$

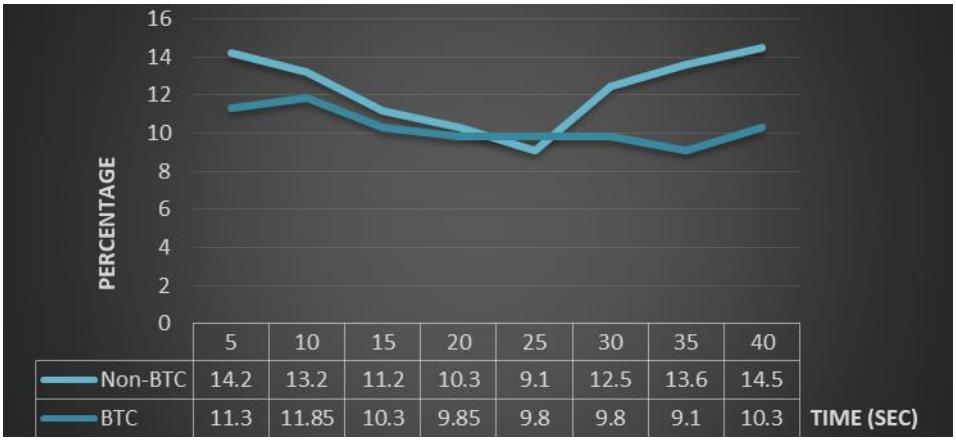

Figure 2 : Drop rate of proposed system with BTC and Non-BTC

2. Throughput:

It is defined as the total number of packet delivered over the total simulation time. It is a ratio of total number of packet received in TCP and total number of packet sent. The broad importance of the output determines the best performance of the protocol.

$$Throughput = \left(\frac{\sum_{i=0}^{k} received\ packet[TCP]}{\sum_{i=0}^{l} sent\ packet[TCP]}\right) * 100$$

ISSN: 2233-7857 IJFGCN

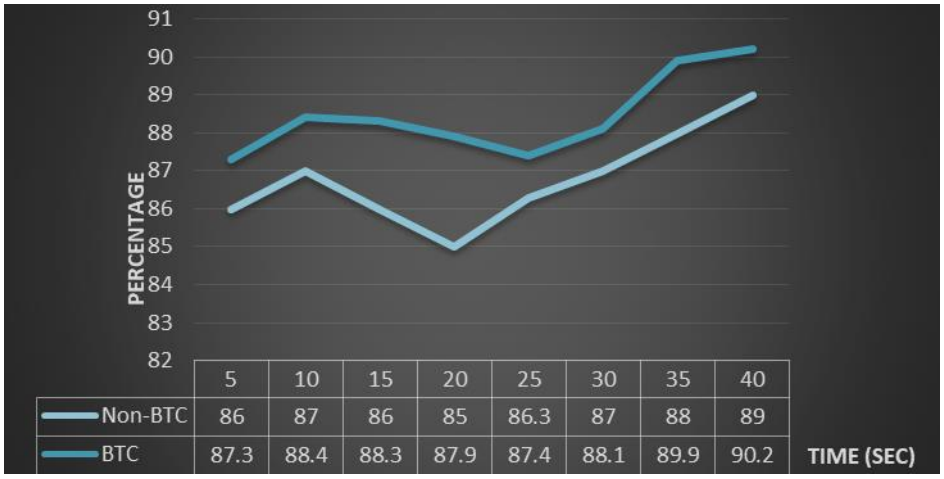

Figure 3 : Throughput of proposed system with BTC and Non-BTC

3. Packet Delivery Ratio (PDR):

Packet delivery ratio (PDR) is defined as the ratio of the number of data packets to the number of packets created by the network. The high value of the packet transmission ratio indicates the optimal performance of the protocol.

$$PDR = \sum_{i=0}^{n} \left(\frac{packet\ received\ [TCP]}{packet\ sent\ [TCP]} \right) * 100$$

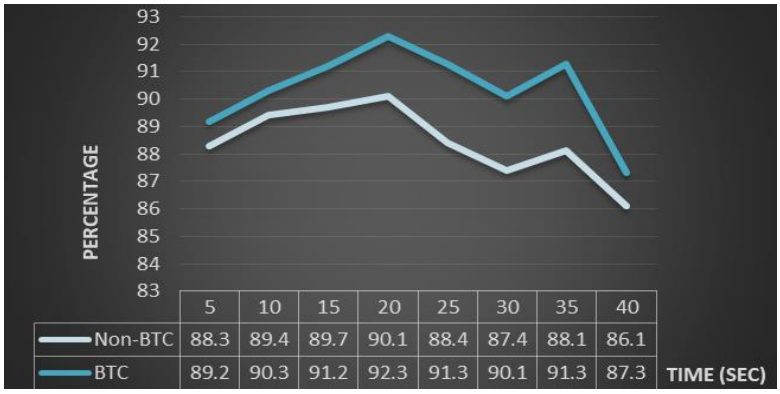

Figure 4 : Packet delivery rate of proposed system with BTC and Non-BTC

In order to know the efficiency of the proposed system, these parameters were evaluated and tracked for various nodes and at different simulation times.

ISSN: 2233-7857 IJFGCN

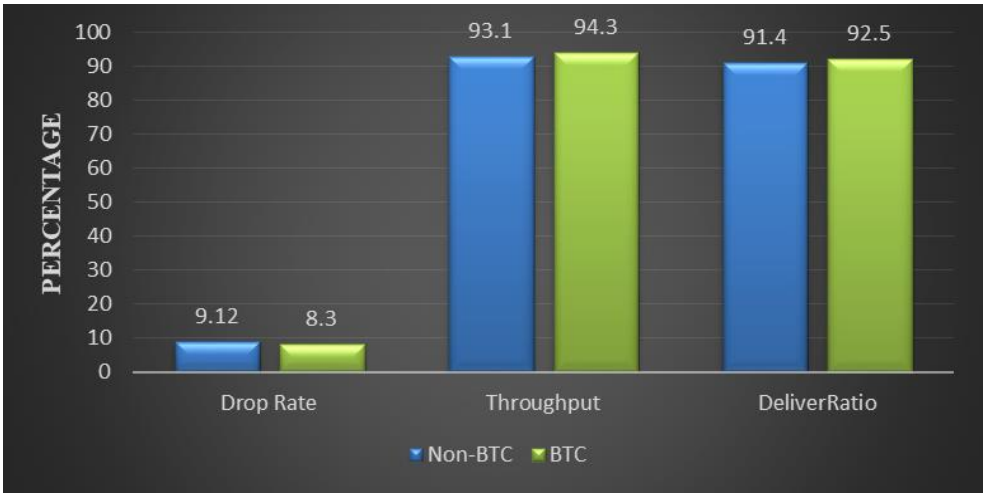

Figure 5: Performance with BTC and Non-BTC

5. CONCLUSION

The SDN gives us the capacity to perform the intended task only by a particular nodes on a network and different for some other nodes and be centrally monitored and managed. With the help of WSN it can collect the wireless data from a remote node and manage it with SDN but with this the issue of quality needs to be resolved is what done by improving the quality of the network. We added two cluster head instead of the traditional one cluster head and removed the bottleneck issue, even though the cluster head failed other was active to contentiously keep the network working and keep the data transmitting from the sourced node to the destined sink node. We monitored out simulation in three different conditions which included the cluster head being dead, the cluster head moving to sleep mode due to low energy or an attack being going on near a cluster head and path node (we considered the flooding attack in our case). In all this condition one of our nodes was failed but then the other came up active and the data was then moved to the sink node by that path so that no communication gap or data drop occurs.

In future there can be more improvement in the quality not just by increasing the number of cluster heads but the consideration of security factors also. We used AODV protocol also other can be used and compared. But in case of the quality improvement our simulation network is better than the others increasing the performance as we used BTC while comparing to Non-BTC networks.

REFERENCES

1. Hu, F.; Hao, Q.; Bao, K. A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation. IEEE Commun. Surv. Tutor. 2014, 16, 2181–2206.
2. Luo, T.; Tan, H.P.; Quek, T.Q.S. Sensor OpenFlow: Enabling Software-DefinedWireless Sensor Networks. IEEE Commun. Lett. 2012, 16, 1896–1899.
3. Costanzo, S.; Galluccio, L.; Morabito, G.; Palazzo, S. Software Defined Wireless Networks: Unbridling SDNs. In Proceedings of the 2012 European Workshop on Software Defined Networking, Darmstadt, Germany, 25–26 October 2012; pp. 1–6.
4. Galluccio, L.; Milardo, S.; Morabito, G.; Palazzo, S. SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, Hong Kong, 26 April–1 May 2015; pp. 513–521.
5. Gante, A.D.; Aslan, M.; Matrawy, A. Smart wireless sensor network management based on software-defined networking. In Proceedings of the 2014 27th Biennial Symposium on Communications (QBSC), Kingston, ON, Canada, 1–4 June 2014; pp. 71–75.

ISSN: 2233-7857 IJFGCN

6. Olivier, F.; Carlos, G.; Florent, N. SDN Based Architecture for Clustered WSN. In Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Blumenau, Brazil, 8–10 July 2015; pp. 342–347.
7. De Oliveira, B.T.; Margi, C.B.; Gabriel, L.B. TinySDN: Enabling multiple controllers for software-defined wireless sensor networks. IEEE Lat. Am. Trans. 2015, 13, 3690–3696.
8. Tootoonchian, A.; Ghobadi, M.; Ganjali, Y. OpenTM: Traffic matrix estimator for OpenFlow networks. In Proceedings of the International Conference on Passive and Active Network Measurement, Zurich, Switzerland, 7–9 April 2010; Springer: Berlin, Germany, 2010; pp. 201–210.
9. Jain, R.; Paul, S. Network virtualization and software defined networking for cloud computing: A survey. IEEE Commun. Mag. 2013, 51, 24–31.
10. Zhou, J.; Jiang, H.;Wu, J.;Wu, L.; Zhu, C.; Li,W. SDN-Based Application Framework forWireless Sensor and Actor Networks. IEEE Access 2016, 4, 1583–1594.
11. Capelle, M.; Abdellatif, S.; Huguet, M.J.; Berthou, P. Online virtual links resource allocation in Software-Defined Networks. In Proceedings of the 2015 IFIP Networking Conference (IFIP Networking), Toulouse, France, 20–22 May 2015; pp. 1–9.
12. Rahmani, R.; Rahman, H.; Kanter, T. Context-Based Logical Clustering of Flow-Sensors-Exploiting HyperFlow and Hierarchical DHTs. In Proceedings of the 4th International Conference on Next Generation Information Technology, Jeju Island, Korea, 18–20 June 2013; Elsevier: Atlanta, GA, USA, 2013.
13. Rahmani, R.; Rahman, H.; Kanter, T. On Performance of Logical-Clustering of Flow-Sensors. arXiv 2014, arXiv:1401.7436.
14. Zhu, Y.; Zhang, Y.; Xia, W.; Shen, L. A Software-Defined Network Based Node Selection Algorithm in WSNLocalization. In Proceedings of the 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, China, 15–18 May 2016; pp. 1–5.
15. Aleksander, M.B.; Dubchak, L.; Chyzh, V.; Naglik, A.; Yavorski, A.; Yavorska, N.; Karpinski, M. Implementation technology software-defined networking in Wireless Sensor Networks. In Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),Warsaw, Poland, 24–26 September 2015; Volume 1, pp. 448–452.
16. Cao, C.; Luo, L.; Gao, Y.; Dong,W.; Chen, C. TinySDM: Software Defined Measurement inWireless Sensor Networks. In Proceedings of the 2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Vienna, Austria, 11–14 April 2016; pp. 1–12.

ISSN: 2233-7857 IJFGCN