RESEARCH PROPOSAL SAMPLE FORMAT

A NOVEL THREE-TIER ARCHITECTURE FOR SECURE AND QOS GUARANTEED SOFTWARE DEFINED WSN IN IOT ENVIRONMENT

STUDENT NAME: Type your name here

STUDENT NUMBER: Enter your student number

COURSE NAME:

DEPARTMENT:

COURSE CODE:

SUPERVISOR: Type your supervisor's name here

DATE OF SUBMISSION: DD MMMM 20YY

ABSTRACT

Background: Software Defined Networking (SDN) is an emerging technology that supports high scalability and refines the traditional networks. With the advancements, SDN has been integrated with many other networks to improve scalability and quality of service (QoS). In upcoming Internet of Things (IoT) applications, Wireless Sensor Network (WSN) will play pivotal role. To address this proliferation in IoT and WSN, this research work uses SDN.

Methods: To alleviate security issues and to improve QoS, novel three-tier architecture is designed in which SDN is integrated with WSN for IoT applications. In each tier, security and QoS is ensured with novel mechanisms and methodologies as,

- For managing large scale network, sensor nodes are segregated into multiple clusters with secure verification. Secure hash functions are operated to authenticate sensor nodes for cluster formation.
- The sensed data is transmitted to sink node via transmission paths which is selected optimally by a new Harris Hawks Optimization algorithm. In route selection, trust value and QoS factors are considered as objective function.
- Sensory data collected from IoT environment is secured by using novel cryptographic primitive namely Parallel SALSA20 algorithm.
- Optimal switch selection for data transmission between sensor nodes and sink node is performed by Artificial Neuro Fuzzy (ANN-Fuzzy) model in which both security and QoS parameters are considered

Results: The proposed three-tier architecture is evaluated in IoT Smart City application based on QoS (PDR, Throughput, Loss Rate, E2E Delay) and security parameters (Security Level, Key Generation Time, Attack Rate, Energy Consumption).

Discussion and Conclusion: From the experiment results, we proved that proposed three-tier architecture is suitable for IoT applications to provide security and QOS.

Keywords- SDN, WSN, IoT, Security, Quality of Service, Parallel Encryption, Hash Function.

INTRODUCTION

SDN is a new networking architecture in which the data plane is decoupled from control plane to serve flexible network management. WSN is the foundation for many IoT applications including Smart City, Smart Healthcare, Smart Environment, IoV and so on. However, in the perspective of IoT, WSN lacks with poor scalability and QoS since in IoT there will be millions of smart sensors are deployed. Managing this huge sensor network, conventional WSN demands a novel architecture. Thus Software Defined Wireless Sensor Network (SDWSN) is introduced which is the proliferating paradigm that brings scalability, flexibility, and better network management in traditional WSN [1], [2]. However, integration of SDN and WSN will improve scalability but introduces some issues such as security threats and QoS management. For improving QoS in the network, Clustering [4], and Routing [3], [5] are widely adapted in SND and WSN. In cluster formation, network is segregated into multiple small clusters which improve network management (i.e.) data sensed by each sensor is transmitted to sink via cluster head (CH) node. Thus it is necessary to elect optimal CH before data transmission. The major benefits of cluster formation in SDWSN are: (i) energy consumption minimization, (ii) better network management, and (iii) assured data delivery. Similarly, optimal route selection involves with electing best route between source and destination to ensure: (i) no/low packet loss, (ii) high delivery ratio, (iii) minimized retransmissions, and (iv) reduction in delay.

Another issue of security can be managed by secure route selection and encryption schemes. In IoT environment, increase in number of nodes also increases security threats which must be managed by the network. In order to improve both security and QOS, secure route selection procedure is also carried out in the network [6], [7], [8]. Secure route selection is built upon trust value provided for each senor node based on its behaviour. Secure route selection rely upon two criteria as: QoS factor and security factor. Along with secure routing, network coding schemes, cryptography schemes, and hashing functions also ensure high-level security in network environment. Involvement of secure routing protects the data transmission from many security threats in the network.

LITERATURE REVIEW

Reference 1

Title: Software Defined Wireless Sensor Networks Application Opportunities for Efficient Network Management: A Survey

Concept

Software defined networking is combined with wireless sensor network to design software defined wireless sensor network. SDWSN improves the network in terms of performance as well as scalability. SDN resolves many issues in WSN and improves the performance of WSN. However, integration of SDN and WSN also involves with some challenges such as QoS and security.

Reference 2

Title: An SDN-assisted Framework for Optimal Deployment of MapReduce Functions in WSNs

Concept

This paper discusses the advantage of SDN in WSN. In this paper, a SDN assisted framework is designed to achieve optimal deployment of map-reduce function in WSN. The network is separated into data plane and control plane. Here the data plane comprises sensor nodes which are responsible for packet forwarding whereas the control plane comprises a controller. The controller has the global view of the network that helps to control the entire network.

Reference 3

Title: Flexible network management and application service adaptability in software defined wireless sensor networks

Concept

In this paper, SDWSN network is implemented with discrete event simulation and a highly extensible scalable SDN controller-Open Daylight. This paper adapts SDN in WSN in order to improve traffic flow routing without increase in transmission delay. In this approach, different levels of flexibility have been achieved with the case of different SDN services such as remote access, network device management, and simple updates. In the underlying network, service chaining functionality is adapted to enable communication among nodes

Reference 4

Title: Energy Efficient Clustering Algorithm for Multi-Hop Wireless Sensor Network Using Type-2 Fuzzy Logic

Concept

To eliminate drawback of type-1 fuzzy system based CH selection, this paper proposes a CH selection method using type-2 fuzzy logic system. Here remaining energy of node, distance between node and BS, and concentration of node are considered as membership functions in fuzzy logic. Type-2 fuzzy system is comprised with four components such as fuzzifier, fuuzification module, type reducer, and knowledge base. In this method, standby CH is selected to rotate CH when energy level of CH was reduced.

Limitation

- ✓ Even this method handle uncertainty by type-2 logic, this method is not able to consider all significant metrics for CH selection.
- ✓ Since standby CH was selected initially, the energy consumption of standby CH was high.

Reference 5

Title: An Innovative MapReduce-Based Approach of Dijkstra's Algorithm for SDN Routing in Hybrid Cloud, Edge and IoT Scenarios

Concept

This paper adapts MapReduce approach to perform routing in SDN networks in IoT/cloud applications. In MapReduce based routing approach, Dijkstra algorithm is utilized for shortest path selection. Thus this paper designs a revised MapReduce version of Dijkstra algorithm for optimal route selection. The entire network is considered as a graph with vertex and edges. In Map phase, key value pairs are generated in which key is given as source vertex and value represents the minimum distance value. The Reduce phase applies Dijkstra algorithm and finds optimal path with minimum distance.

Limitation

- ✓ In general, Dijkstra algorithm is involved with large time consumption and it is not able to handle negative edges which lead to non-optimal path selection. Thus shortest path selection by Dijkstra algorithm is not suitable to find optimal route
- ✓ Route selection based only on distance is efficient

Reference 6

Title: STAR: Preventing Flow-table Overflow in Software-Defined Networks

Concept

This paper proposes a SofTware-defined Adaptive Routing (STAR) scheme in order to mitigate flow table overloading attack in SDN. This method proposed a routing scheme in order to improve the utilization of limited flow table resources. In this manner, the network performance is improved. In STAR method, unused flow entries are evicted to mitigate the flow table overloading problem. SDN controller is involved with routing decision module and functions of this module are admission control and flow-table utilization aware routing. New flow entries are accepted at switches if the flow table utilization of that switch was minimum.

Limitation

- ✓ This method is limited to certain packet types and not able to support all types of packets
- ✓ Route selection is not efficient in this method

Reference 7

Title: ActiveTrust: Secure and Trustable Routing in Wireless Sensor Network

Concept

An active trust routing protocol for secure routing in sensor networks is presented in this paper. This protocol is tried to detect black hole attack in networks quickly by using the trust values of nodes. Active trust algorithm significantly improves the data route access probability and ability to detect a black hole. Trust value is computed in terms of nodal direction trust, nodal recommendation trust, and comprehensive trust.

Limitation

- ✓ Hereby path selection is performed by selecting high trusted node that is placed nearly to sink which increases difficulties in routing.

Reference 8

Title: A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network

Concept

This paper presents a secure routing method based on trust value of sensor node. In this method, each node in the network is included with trust evaluator, trust data base, route resolve, and route setup. Trust evaluator is responsible for classifying neighbor nodes into trusted node, malicious node, and faulty node. Route selection considers both trust factor energy efficiency. Route with only trusted nodes and high available energy is selected as optimal route.

Limitation

- ✓ Involvement of four modules at each sensor increases space complexity
- ✓ Classification of nodes at each route selection increases computation overhead at sensor nodes.

Reference 9

Title: A Lottery SMC Protocol for the Selection Function in Software Defined Wireless Sensor Networks

Concept

This paper proposes a lottery secure multiparty computation (SMC) protocol for improving data security in SDWSN. The proposed lottery-SMC protocol is performed based on layered homomorphic encryption and the equivalent transformation of two-arrays. The lottery-SMC protocol is adapted for the selection function.

Limitation

- ✓ Not able to protect the network from malicious nodes

Reference 10

Title: A Software Defined Network Routing in Wireless Multihop Network

Concept

A multi-hop wireless routing protocol is proposed in this paper based on SDN. In the SDN based wireless multi-hop network, SDN controller is deployed to maintain the global view of the network and to select optimal single path or multiple paths for data transmission. The shortest path selection considers energy and hop count. The controller update information of nodes by exchanging control packets such as CON-INFO, NODE-INFO, REQ, REQ-ACK, UPDATE, and STAT.

Limitation

- ✓ This network suffers from single node failure problems since control plane is involved with single controller
- ✓ Route selection based only on energy and hop count increases transmission time for data transmission
- ✓ Multiple control packet exchange between node and controller increases energy consumption

Reference 11

Title: A ReRAM Physically Unclonable Function (ReRAM PUF)‐Based Approach to enhance Authentication Security in Software Defined Wireless Networks

Concept

This paper proposes an authentication scheme based on physical unclonable functions (PUFs). In this paper, digital PUFs are developed using inherent randomness of the nanomaterials of resistive random access memory (ReRAM). PUFs are hardware primitive that are embedded in most of the IoT devices in order to enable secure authentication and access control in the network. In addition, PUF based public key infrastructure (PKI) protocol also proposed to secure the controller in SDWSN.

Limitation

- ✓ However, PUFs are hardware primitives which require modifications in the sensor devices to achieve security

Reference 12

Title: PUF-Assisted Group Key Distribution Scheme for Software-Defined Wireless Sensor Networks

Concept

This paper proposes a group key distribution scheme for SDWSN using PUFs. Here PUFs are adapted for security provision since they are difficult to be cloned, and predicted. In SDWSN, the PUF challenge is stored in the sensor device. Here ring oscillator (RO) PUF based on signal transmission delay is adapted. The control plane is designed with two controllers such as main controller and auxiliary controller.

Limitation

- ✓ However, PUFs are hardware primitives which require modifications in the sensor devices to achieve security

Reference 13

Title: A Secure Network Coding Based on Broadcast Encryption in SDN

Concept

This paper proposes a broadcast encryption scheme to secure SDN from attackers. In this approach, intermediate nodes which received the data were allowed to encode the data in order to strengthen the security level. Encoding is performed by secure switch network coding multicast (SSNC). Here data layer is comprised with users and switches and each device connected in the data layer is authenticated before enter into the network. Then multicast packets are separated and aggregated.

These aggregated multicast packets are transmitted through secure route selected by controller. Through this route, multicast packets are transmitted in network coding manner.

Limitation

- ✓ Encoding and decoding at each intermediate node increase overhead and time consumption in the entire network.

Reference 14

Title: A dynamic-scheduling mechanism of controllers based on security policy in software-defined network

Concept

In this paper, MaxSG SDN architecture is proposed with the aim of improving security aspects in the network. Major objective of this work is to develop a security system to secure controllers in network operating system (NOS). Here the diversity is altered to maximum degree in order to improve security gain through scheduling approach. This scheduling problem is formulated as NP-hard problem and solved by heuristic algorithm.

Limitation

- ✓ However, this method is only able to secure control plane and not able to secure data plane.

Reference 15

Title: Water rippling shaped clustering strategy for efficient performance of software defined wireless sensor networks

Concept

This paper proposes water rippling shaped clustering (WARIS) algorithm for cluster formation in large-scale software defined wireless sensor network. The WARIS algorithm is designed based on the shape of water rippling. In addition, energy aware cluster head (CH) selection is performed to improve clustering performance and to reduce re-clustering overhead. For CH selection the energy consumption due to intra-cluster communication, inter-cluster communication, and data processing are considered. The algorithm is initiated by base station and the cluster size is optimized.

Limitation

- ✓ CH selection is not efficient since single metric is considered
- ✓ In re-clustering phase, the CH selection is performed within specific area which leads to ineffectual CH selection

PROBLEM STATEMENT

In SDWSN environment, joint security and QoS provisioning is challenging since the network design includes various elements viz. sensor nodes, SDN switches, sink node, and controller. Many research works has been proposed in recent times regarding security and QOS issues in SDWSN. However, none of the works is able to address both security and QOS jointly.

Optimal routing based on traffic load is proposed for achieving better QoS in SDWSN environment [16]. At first, the number of forwarding areas and number of forwarders in each area is predicted. Then the predicted numbers of optimal forwarders are selected based on node identity degree. Herein node identity degree is computed upon the similarity level between packets of both nodes. Finally, the flow is divided into multiple segments and each segment is transmitted through each forwarding nodes.

Problems Stated

This work has some drawbacks:

(i). Leads to large number of packet loss since forwarder selection is performed based only on similarity level

(ii). Further there will be no change is load due to splitting mechanism rather than time consumption. Because, Here similarity is determined before flow splitting, and then the divided segment is transmitted to forwarder to minimize the load

(iii). Increased number of forwarders and number of segments in flow results in large packet loss which will not able to assure QoS

For QoS improvement, congestion management mechanism is discussed [17]. For that an open-flow based active network management (OF-ANM) strategy is designed. Here OF-ANM collects the link state information such as list of one-hop neighbors, queue length, packet arrival rate, and residual energy from each node. Then the flow-rate rate for each node is computed to improve QoS. When flow arrival rate of a sensor node exceeds the limit, then the controller redirects the flows towards other node to avoid congestion.

Problems Stated

(i). SDWSN design with single controller leads to single node failure which degrades the performance of entire network

(ii). Flow diverting to another nodes without considering significant metrics further increases network congestion

In SDWSN, controller is responsible to select appropriate route between source and destination [18]. For optimal route identification, Dijkstra based shortest path selection algorithm is adapted. Residual energy and hop count metrics are considered for optimal route selection. The nodes update the information to controller by exchanging following control messages: NODE INFO, RREQ, RACK, UPDATE, STAT and so on.

Problems Stated

(i). Energy consumption and bandwidth consumption is large due to information exchange between each node and controller

(ii). Suffers from single node failure problem

(iii). Route selection based on limited metrics is not able to ensure the efficient data delivery

In SDWSN based smart city application, chance discovery and usage control theory are proposed for security provision [19]. Attack detection is performed in two levels: (i) sensor level, and (ii) sink level detection. In sensor level (i.e.) low level detection, keygraph based chance discovery algorithm is used. In sink level (or) high level attack detection, keygraph is utilized with data crystallization scheme.

Problems Stated

(i). Construction and updation of keygraph in each sensor node increases time consumption as well as complexity

(ii). In this detection method, the event with small frequency of occurrence is considered as attack which is not accurate.

Privacy preserving cross-domain routing optimization (PYCRO) algorithm is built upon Quick Pathing Technique [20]. Here shortest path is selected based on policy-compliant in which user privacy protection is ensured. In PYCRO algorithm, equivalent graph construction and privacy preserving shortest path tree protocol is involved. Path tree was constructed on equivalent graph

constructed at first stage. After path selection, data transmission is carried out through that optimal path in encrypted form. In this approach, homomorphic encryption algorithm is utilized to encrypt data.

Problems Stated

(i). PYCRO algorithm is not suitable for network with dynamic topology since dynamic topology require frequent construction of path tree.

Research Question/Hypothesis

Now we pose the number of questions regarding security and QoS provision in SDWSN environment for IoT applications.

- ✓ How to design SDWSN architecture that apt for IoT applications?
- ✓ How to manage the network and to find the unauthorized nodes?
- ✓ How to select appropriate route for data transmission?
- ✓ How to secure the transmitted data between source and destination?

Research Objectives

This research work is aimed to resolve the problems discovered from prior research works. The major objectives formulated are,

- ✓ Designing novel SDWSN architecture for IoT applications
- ✓ To secure network from malicious and unauthorized nodes via strong authentication
- ✓ To ensure QoS in data transmission by selecting optimal route between source and destination
- ✓ To secure the data from malicious nodes with better encryption scheme

RESEARCH DESIGN AND METHODS

To resolve all prior research problems and to grasp research objectives, this work designs novel three-tier SDWSN architecture for IoT applications. Design of three-tier architecture is organized as follows,

- ✓ **IoT Sensor Tier**- Includes IoT sensor nodes that are deployed for dedicated objective and authentication server. Data is generated from this tier and reaches sink node for further analysis
- ✓ **OpenFlow Switches Tier**- Includes numbers of OpenFlow Switches which forward the huge volume of data generated IoT tier to next-tier. All OFSs are working upon flow rules deployed by controller
- ✓ **Controller Tier**- Includes multiple SDN controllers and sink nodes. Controllers are responsible to maintain global view of the entire network and to modify flow rules according to network status.

Major objective of three-tier SDWSN is to achieve "**Improved QoS without loss in Security**". This objective is attained by,

SECURE CLUSTER FORMATION

Sensor nodes presented in IoT Sensor Tier are segregated into multiple clusters and in each cluster an optimal CH is selected. Initially, each sensor node is authenticated at authentication server using ***ID, Password, and Location*** using hash function. For hashing operation, **Blake-256** algorithm is used. Node which passes authentication process successfully is provided with a secret code which is used in cluster formation. Optimal CH is selected based on *Residual Energy, Distance with OFS Tier, and Mobility*. Then the clusters are formed by verifying the secret code of each node which is obtained from AS. In this phase, all unauthorized nodes are identified and secure clusters are formed.

OPTIMAL ROUTE SELECTION

When a node has sensory data, then the data must be transmitted to sink node via CH. To enable optimal routing between source node and CH, **Harris Hawks optimization (HHO)** algorithm is proposed. In HHO algorithm, ***QoS factor (Energy Level, Distance, Mobility) and security factor***

(Direct Trust Value, Indirect Trust Value, Belief Level) are considered for objective function formulation. Proposed HHOP algorithm works better for optimization problems and convergence is lower than conventional algorithms.

DATA SECURITY

The sensed data aggregated by CH is then encrypted to protect from malicious nodes. For ensuring high-level security **Parallel SALSA20** cryptography scheme is proposed. Using Parallel SALSA20 algorithm minimizes energy consumption since SALSA20 is lightweight cryptography and also minimizes time consumption. Then the data is transmitted to sink node via OFS in encrypted format.

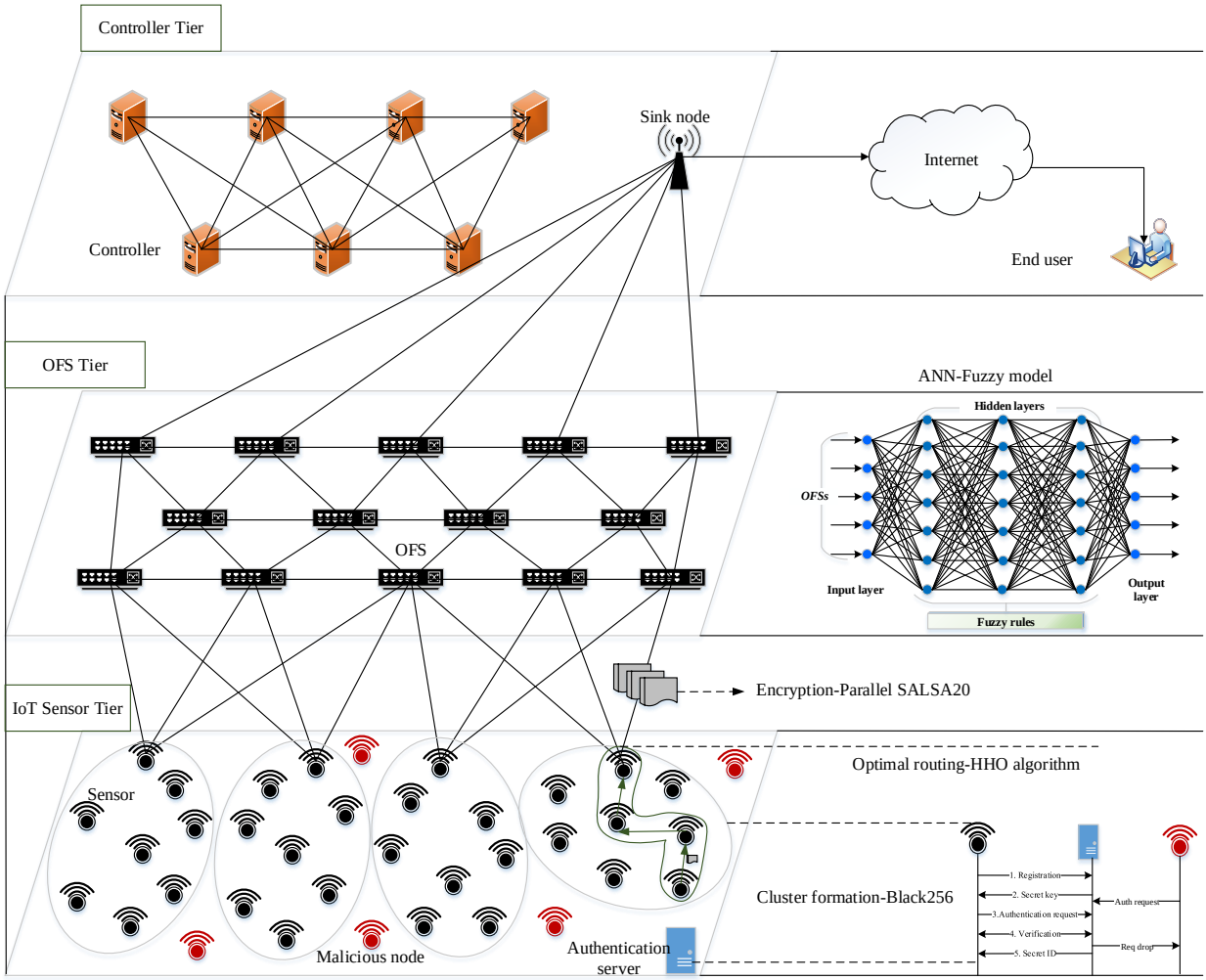
OPTIMAL OFS SELECTION

In the presence of vast number of sensor nodes, the volume of data generated by IoT sensor tier is also huge which increases load in OFS tier. To balance load in OFS Tier and to improve data transmission, optimal OFS selection is carried out by CH. For optimal OFS selection, **ANN-Fuzzy** model is proposed. Here Current Load of OFS, distance with OFS, and Trust value of OFS are considered in ANN-Fuzzy model in which optimal rules are deployed for OFS selection.

RULES DEPLOYED IN ANN-FUZZY MODEL

Input			**Output**
Current load	**Distance with OFS**	**Trust value**	
Low	Low	Low	Partially Optimal OFS
Low	Low	High	Optimal OFS
. . .	. . .	. . .	. . .
High	High	High	No Optimal OFS

SYSTEM ARCHITECTURE



EXPECTED OUTCOMES AND DISCUSSION

The major objective of this research work is to achieve QoS and security in SDWSN for IoT applications. To evaluate the performance of this work, the proposed three-tier architecture is modelled experimentally in network simulator tools and expected to achieve better results in terms of,

- ✓ QoS Parameters
  - PDR
  - Throughput
  - Loss Rate
  - E2E Delay
- ✓ Security Parameters
  - Security Level
  - Key Generation Time
  - Attack Rate
  - Energy Consumption

REFERENCES

[1] Kgotlaetsile Mathews Modieginyane, Babedi Betty Letswamotse, Reza Malekian and Adnan M. Abu-Mahfouz, "Software Defined Wireless Sensor Networks Application Opportunities for Efficient Network Management: A Survey", Computers and Electrical Engineering, Elsevier, Vol 66, pp 274-287, 2018.

[2] Kgotlaetsile Mathews Modieginyane, Reza Malekian, Babedi Betty Letswamotse, "Flexible network management and application service adaptability in software defined wireless sensor networks", Journal of Ambient Intelligence and Humanized Computing, Springer, pp 1-10, 2018.

[3] Angelos-Christos G. Anadiotis, Giacomo Morabito, and Sergio Palazzo, "An SDN-assisted Framework for Optimal Deployment of MapReduce Functions in WSNs", IEEE Transactions on Mobile Computing, Vol 15, No 9, pp 2165-2178, 2016.

[4] Padmalaya Nayak, Bhavani Vathasavai, "Energy Efficient Clustering Algorithm for Multi-Hop Wireless Sensor Network Using Type-2 Fuzzy Logic", IEEE Sensors Journal, Vol 17, No 14, pp 4492-4499, 2017.

[5] Alina Buzachis, Antonino Galletta, Antonio Celesti, and Massimo Villari, "An Innovative MapReduce-Based Approach of Dijkstra's Algorithm for SDN Routing in Hybrid Cloud, Edge and IoT Scenarios", Service-Oriented and Cloud Computing, Springer, Vol 185-198, 2018.

[6] Zehua Guo, Ruoyan Liu, Yang Xu, Andrey Gushchin, Anwar Walid, H.Jonathan Chao, "STAR: Preventing Flow-table Overflow in Software-Defined Networks", Computer Networks, Elsevier, Vol 125, pp 15-25, 2017.

[7] Yuxin Liu, Mianxiong Dong, Kaoru Ota, Anfeng Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Vol 11, No 9, pp 2013-2027, 2016.

[8] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Abdul Waheed Khan, "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network", Mobile Networks and Applications, Springer, Vol 21, No 2, pp 272-285, 2016.

[9] Yi SUN, Zhaowen LIN, Yan MA, "A Lottery SMC Protocol for the Selection Function in Software Defined Wireless Sensor Networks", IEEE Sensors Journal, Vol 16, No 20, pp 7325-7331, 2016.

[10] Junfeng Wang, Yiming Miao, Ping Zhou, M. Shamim Hossain, Sk Md Mizanur Rahman, "A Software Defined Network Routing in Wireless Multihop Network", Journal of Network and Computer Applications, Elsevier, Vol 85, pp 76-83, 2017.

[11] Fatemeh Afghah, Bertrand Cambou, Masih Abedini, Sherali Zeadally, "A ReRAM Physically Unclonable Function (ReRAM PUF)‐Based Approach to Enhance Authentication Security in Software Defined Wireless Networks", International Journal of Wireless Information Networks, Springer, Vol 25, No 2, pp 117-129, 2018.

[12] Meigen Huang , Bin Yu, and Sensen Li, "PUF-Assisted Group Key Distribution Scheme for Software-Defined Wireless Sensor Networks", IEEE Communication Letters, Vol 22, No 2, pp 404-407, 2018.

[13] Yue Chen, Hongyong Jia, Kaixiang Huang, Julong Lan, and Xincheng Yan, "A Secure Network Coding Based on Broadcast Encryption in SDN", Mathematical Problems in Engineering, 2016.

[14] Chao Qi, Jiangxing Wu, Hongchao Hu and Guozhen Cheng, "A dynamic-scheduling mechanism of controllers based on security policy in software-defined network", Electronics Letters, Vol 52, No 23, pp 1918-1920, 2016.

[15] Syed Bilal Hussian Shah, Zhe Chen, Fuliang Yin, Awais Ahmad, "Water rippling shaped clustering strategy for efficient performance of software define wireless sensor networks", Peer-to-Peer Networking and Applications, Springer, pp 1-10, 2017.

[16] Guozhi Li, Songtao Guo, Yang Yang and Yuanyuan Yang, "Traffic Load Minimization in Software Defined Wireless Sensor Networks", IEEE Internet of Things Journal, Vol 5, No 3, pp 1370-1378, 2018.

[17] Babedi Betty Letswamotse, Reza Malekian, Chi-Yuan Chen, Kgotlaetsile Mathews Modieginyane, "Software defined wireless sensor networks and efficient congestion control", IET Networks, Vol 7, No 6, pp 460-464, 2018.

[18] Junfeng Wang, Ping Zhai, Yin Zhang, Lei Shi, Gaoxiang Wu, Xiaobo Shi, and Ping Zhou, "Software Defined Network Routing in Wireless Sensor Network", Cloud Computing, Security, Privacy in New Computing Environments, Springer, pp 3-11, 2017.

[19] Jun Wu, Kaoru Ota, Mianxiong Dong and Chunxiao Li, "A Hierarchical Security Framework for Defending against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, Vol 4, pp 416-424, 2016.

[20] Qingjun Chen, Shouqian Shi, Xin Li, Chen Qian, Sheng Zhong, “SDN-based Privacy Preserving Cross Domain Routing”, IEEE Transactions on Dependable and Secure Computing, 2018.