# Utilising Artificial Intelligence in Software Defined Wireless Sensor Network

Omolemo Godwill Matlou
Department of Electrical Engineering
Tshwane University of Technology
Pretoria, 0001
South Africa
Email: 217626978@tut.ac.za

Adnan M. Abu-Mahfouz
Department of Electrical Engineering
Tshwane University of Technology
and
Meraka Institute, CSIR
Pretoria, South Africa

***Abstract*—Software Defined Wireless Sensor Network (SDWSN) is realised by infusing Software Defined Network (SDN) model in Wireless Sensor Network (WSN), Reason for that is to overcome the challenges of WSN. Artificial Intelligence (AI) and machine learning play an important role in our society, give rise to systems that can manage themselves. WSNs have been used in various industrial applications, where reliability and network performance are critical success factors. Many advanced AI techniques can be utilised to improve the performance and reliability of these applications. Investigating the AI algorithms applied to SDN may bring improved network management, security or routing in SDWSN which may result in a more reliable network. We look at machine learning algorithms applied in SDN and discuss the possibility of using these AI in SDWSN to address the WSN challenges and improve its performance and reliability.**

***Keywords—AI; WSN; SDN; SDWSN;Machine learning; security; routing; traffic management***

## I. INTRODUCTION

Wireless sensor Networks (WSNs) have the potential to build powerful applications [1]–[7], each with their own characteristics and requirements. WSN comes with many design requirement such as data aggregation, localisation, energy-aware routing, data reliability, node clustering, event scheduling, security and fault detection [8]–[14]. Energy challenge in WSN is mainly due to radio communication, which involves data transmission and reception. Routing is another issue when it comes to WSN, the three major driving forces for efficient routing techniques are: 1) need for Quality of Services (QoS) guaranteed 2) Newly deregulated telecommunications industries and 3) Explosives growth in network size and usage [15].

WSN security is another issue , WSN attacks are classified in three categories: 1) Goal-oriented (passive and active attacks), 2) Performer-oriented (outside and inside attack) and 3) Layer-oriented (target layers of the network stack, physical layer or MAC layer) [16].

With these challenges to WSN and considering the growing need of WSNs applicable devices and Internet of Thing (IoT) devices hitting the market, these challenges needs solution, many researchers have listed Software Defined Network (SDN) as the potential solution to WSN challenges [17], [18]. SDN is defined as a framework to allow network administrators to automatically and dynamically manage and control many network devices. SDN also allows physical separation of the control plane from the forwarding plane in the network [19].

Reasons why SDN is needed, virtualisation (using network resource without worrying where its located), Orchestration (ability to manage many devices with one command), programmable (should be able to change behaviour in an instant), dynamic scaling (should be able to change quantity and size), automation, performance (optimise network device and capacity, load balancing and bandwidth management) and service integration (fire walls and intrusion detection system). Application of SDN to WSN gives rise to SDWSN (software defined wireless sensor network). Importance of SDN in WSN are given in [17], where the authors outline solution to the challenges in WSN based on SDN where functions that consumes energy will reside in the controller, which has enough power resources. SDN also provides solution to routing, mobility, and localisation in WSN by letting the controller manage them. Furthermore, SDN can be utilised to provide a better management of large scale WSN [20]

The application of SDN to WSN does answer a lot of the challenges faced in WSN but even with these solutions, researchers are always looking for other means to further manage challenges and come up with solutions to improve energy and power consumption, come up with efficient approaches to routing in the networks and approaches to security of this network. Recently researchers have considered using AI in SDWSN to approach energy saving, improve routing and security in SDWSN. Many scientists use machine learning as a technique for AI. AI or machine learning are important in WSN mainly because:

- Dynamic environments change over time and sensor nodes are used to monitor these changes, sensor nodes must adapt and operate efficiently.
- Data is sometimes gathered in locations that are unreachable, dangerous and unpredictable thus self-calibration network will be essential.

The author of [21] review different applications of AI applied to different parts of SDN mainly routing, security and network management. Bai [22] focused more on network routing problems that can be addressed using AI. However, the focus of this paper will be more in the potential of utilising AI

techniques in SDWSN. Therefore, we review and analyse some of the work done using AI as an approach to SDWSN and highlight some of the existing gaps. Finally, we provide a summary of the discussed algorithms in terms of their application, AI technique used, objectives and remaining challenges.

## II. AI IN ROUTING AND TRAFIC MANAGEMENT

Artificial Intelligence has become an interesting topic in almost all research areas taken by scientist and engineers. It was a topic for the intelligence of machines. In this section, we discuss some of the application that researchers used AI algorithms or techniques as an approach to SDN with an objective to utilize them in SDWSN as well.

### *A. Routing*

Routing provides networks with the ability to transport packets to different nodes depending on where they are required. A routing mechanism must insure that data can travel through the network between arbitrary end points, the network should be able to support: overload situations, heavily and lightly loaded network, fluctuation of traffic patterns [15]. The survey done in [21], introduces the concepts of load balancing function which is the requirement for maximising the throughput and minimising the latency in computer networks to support multiple routing approaches.

Few algorithms based on AI are introduced to approach routing and QoS traffic classification in SDN [21]. Back propagation neural network (BPNN) is used to achieve real time dynamic load balance and has decreased latency by 19.3% compared to other method like static round robin methods. The BPNN is applied internally inside the Open vSwitch and is used to reduce the time consumed for sending routing decision from the controller to the Open vSwitch [23]. Ant Colony Optimization (ACO) is another algorithm that is based on how ants behave to find the best route to get from their food supply to the nest. The SDN application runs ACO algorithms on a weighted graph in the SDN controller, where the weights are the loss rate and delay experienced in each network device. ACO compared to the shortest path algorithm has achieved 24.1% increase for the Quality of Experience (QoE) value [24].

Many of the work done using AI which tackles routing problems falls under the following category of algorithms: shortest path algorithms, algorithmic resource allocation methods and distributed AI and agent based routing [15].

In computer networks QoE measures the value of service provided by the network from the customer perspective. QoS-aware adaptive routing (QAR) in multi-layer hierarchical SDN using Reinforcement Learning (RL) approach is proposed. The proposed algorithm is based on the knowledge that various QoS requirement in packet delay, loss and throughput should be supported by an efficient transportation that goes with each application specified. They introduced an architecture based on the distributed hierarchical control plane that complies with OpenFlow 1.2+. The hierarchical has three levels of distributed controllers, which are the super, domain (or master) and slave controller.

QAR algorithm with the aid of RL is proposed through the examination of long-term revenue, action policy, system model with reward function ad quality function and to realise an efficient adaptive, QoS-provisioning routing, SoftMax action selection policy, start-action-reward-state-action method for quality update and markov decision process with QoS-aware reward function are introduced [25].

The proposed algorithm in [25] outperforms most algorithms when it comes to QoS routing for SDN and the algorithm can be a solution not only to the routing challenge of WSN but also to scalability of the WSN although due to the architecture change the algorithm might need to be adjusted and retested when SDN combines with WSN to form SDWSN.

More work has been done to enhance QoS of routers, the authors in [26] proposed a framework for QoS-aware traffic classification using semi-supervised machine learning. Since SDN proposes the separation of the control and data plane thus we need to revisit and redesign the traffic engineering solutions of SDN so that the features of SDN may be exploited when SDN manages network traffic based on flows, then accuracy and efficiency of the traffic classification (TC) engine plays an important role in SDN. An essential part of the traffic engineering in SDN is to provide desired QoS. It is up to the TC engine to provide QoS class for a traffic flow so that a suitable routing path may be chosen. This becomes a problem when new devices are introduced and it sometimes becomes difficult to identify QoS class of the traffic flows when most may belong to the same QoS class [22], [26].

### *B. Traffic mmanagement*

An efficient algorithm that can identify QoS classes, able to choose an appropriate path even when new applications are introduced thus reducing the need to keep maintaining the real-time update of the list of all applications within the Internet is proposed. The proposed framework consists of two components: 1) local traffic identification component at SD-switches at the network edge and 2) the global traffic classifier at the network controller. This proposed classifier has three advantages: i) the SD-switches are kept as simple as possible by only incorporating lightweight elephant flow identification, ii) network controller is utilised to guarantee the accuracy and the adaptability of the QoS classifier, iii) the whole framework follows a modular design principle so that every component in the framework can be improved at any time. This proposed QoS classification solution can be adopted to enable fine-grained QoS-aware traffic engineering in SDN [21], [26].

The proposed framework in [25], aims to classify a traffic flow into a QoS category in a real-time and adaptive fashion without the need of identifying the exact application from which the traffic flow is generated. The TC engine is in the centralised SDN controller. TC engine performs the following: a) efficient network monitoring with low overhead and minimal switch changes, b) detection of QoS significant flows, c) QoS aware traffic classification, d) enables services such as application detection using Deep Packet Inspection running in the network controller.

This system consists of two main processes; elephant flows detection and statistics collection and features extraction. These

two processes consist of two components. The first component is responsible for detecting the QoS-significant flows in the new incoming flows. The second component performs the QoS aware traffic classification and the related network management. The machine learning algorithm used in this system has the following features which are used to train the network and classify the flows:

- Time information: inter-arrival period
- Packet information
- Protocol information

Since not all data found in the traffic is labelled the algorithms struggles with the unlabelled data. Although the semi-ML purpose is to incorporate both principle of the supervised algorithm and unsupervised algorithms of machine learning hence the name semi-ML. further research in this is needed using principles of supervised and unsupervised machine learning algorithms to SDWSN. Also during the evaluation of the algorithm researched they could not find an accurate way of testing the accuracy of their results since the unlabelled flows cannot be verified with an unknown application after going through the classifier. Therefore, more research is needed to determine the accuracy of unlabelled data from given data testing.

## III. AI IN SECURITY

Compromised network may be used to gain access to sensitive information, implement attacks on other users or bring the internet down thus a secure network connection is always required. With technology becoming more advanced requires fast and reliable network, the security also needs to be improved especially with more threats coming out. Security measures deployed in networks needs to be able to adapt to new threats that is learning from previous threats detected and adapting to coming up with new ways to counter new threats. The ability for network security to be able to learn to adapt to new threats can be introduced using AI and machine learning algorithms. Every threat has a pattern regardless of how new it is thus machine learning is the best approach to this issue.

Security services provided to the network layer in SDN includes flow-control, automated security management decoupling network control and data forwarding function, packet routing, identity authentication, and privacy protection. The network control is enabled by SDN to perform anomaly detection in exploring new threats with OpenFlow protocol. Devices with OpenFlow protocol have network-layer security privacy control mechanism to ensure that information is secure and privacy is ensured, this is done by monitoring network activity and detecting suspicious behaviour in the network.

### *A. Using Support Vector Machine Algorithm*

Wang *et al.* [27] introduced an algorithm to monitor security in SDN by using support vector machine (SVM). SVM is a supervised learning algorithm which is used to analyse data and recognise patterns, mostly used to cluster data. The proposed algorithm focuses on flow management on the network and categorising threats in network intrusion detection system (NIDS). Reason for this approach is to create an algorithm that is capable of monitoring data flow in the network and provide security against threats in SDN. They proposed an improved behaviour-based SVM with learning algorithm which can guarantee efficient flow control and detect threats. To speed up the learning of normal and intrusive patterns and improve accuracy of detecting intrusion of SVM they incorporated Iterative Dichotomiser 3 decision tree theory which will outrank raw features and determine the most qualified features to train SVM-classifier (SVC).To defend against network attacks this process usually involves combination of attack detection, traffic classification and response tools, this aims to block traffic deemed illegitimate and allow legitimate traffic through. The authors [27] implemented information security system which had Open vSwitch, sFlow toolset, and sFlow-RT to collect data from suspicious connections and SVC to identify anomaly traffic flows. Looking at their results the system works well in monitoring the traffic flow and has an increased response time when it comes to threats such as Denial of Service (DoS), Distributed Denial of Service (DDoS), etc.

### *B. Using Semi-supervised Machine Learning Algorithm*

Four machine learning algorithms which were compared with each other are introduced, this machine learning algorithm's aim to improve security in the IDS against DDoS. Attacks are first started at the network layer if that fails then the attacks move to application layer and floods the HTTP GET messages [16], [28]. The proposed model based on the IDS consists of two modules: i) first module is an advanced signature based IDS which processes request and finds out if the hosts has normal or anomalous behaviour, ii) the second module checks packets sent from hosts if they are suspicious. First module is designed using machine learning techniques.

Anomalous behaviour detection uses machine learning techniques again to check packets if they are suspicious before proceeding to transport the packet. If the packet has DDoS attack the system displays which host sent the infected packet and updates the flow table. This method although sufficient with regards to preventing DDoS attacks, the problem with it is that the host which had sent the packet with DDoS will become unusable next time as its address will be added to the list of blocked host and there is no guarantee that the host will send infected packets all the time thus we need a way to improve the algorithm.

Networks have flow tables in switches which show the paths of the packets. OpenFlow has access to these tables as well as the controller. When a packet arrives, OpenFlow switch checks the flow table to find a match, with no match the packet is sent to the controller which performs further processing.

Machine learning algorithms considered are: 1) naïve bayes (conditional probability model, which assigns the class label to given data based on the probability), 2) K nearest neighbour (classifies data based on similarities), 3) K-means (aims to partition data observation into k clustering where each observation belongs to the cluster with the nearest mean), 4) K-medoids (share properties of K-mean). Each of these algorithms is implemented in the IDS.

Looking at the results from the experiments and simulations ran it showed that naïve bayes outperformed the other algorithms by having high accuracy but compared to the other algorithms took time to train data thus if we increase the data it means the training time will also increase. Other machine learning algorithms should be considered to run the same scenario used in this research to compare its results and to determine an algorithm that might save time when it comes to training data. By comparing machine learning algorithms in IDS or NIDS will give us an indication of which algorithm to be implemented in SDWSN is suitable to be used to give us an efficient network security threat monitoring.

## IV. AI IN ADMISSION CONTROL

SDN controller has different tasks and one of the key tasks is the admission control (AC) when request for connection comes through. When the network becomes highly utilised AC controller manages the service request. If resources are available AC accepts request and if not drops the request. AC procedures deployed are threshold-based, they use min, max, exclusive, and non-exclusive limits on resource portion that the network operator can define for different classes of flows.

Defining the threshold is a problem since optimal configuration depends on the network traffic condition, which changes every time. Authors in [29] categories the algorithms used for AC in two i) average-care and ii) worst-case. Worst-case are characterised by max and min performance, where malicious adversary chooses the worst possible sequence of connection request. Average-case performance well but the performance is not guaranteed in specific adversary.

An online meta-algorithm based on past decisions and rewards obtained by different AC algorithms will be capable of tracking and following the advice of the last AC algorithms, but this proves difficult since traffic is unpredictable therefore authors in [29] proposed a strategic expect meta-algorithm (SEA) which select algorithm with an increasing number of consecutive steps and does not revisit its choice at each new connection request. SEA is based on the profit effectively obtained by each algorithm when it has been selected. Expected average performance of SEA is always superior to the single performance achieved by the algorithm sequentially chosen by SEA itself during its play.

SEA was evaluated compared to follow-the-leader meta-algorithm (FLA). It was observed that when an AC best performance FLA takes advice from it but fails to track the best expert while SEA runs on top of three computational efficient online algorithms. SEA outperforms. There is still a lot of work that needs to be done in this domain, more research needs to be taken to find more meta-algorithms capable of efficiently selecting AC algorithms.

## V. AI IN SDWSN

### A. *Energy-effcicient routing algorithm Using Reinforcement Learning*

Most work done on SDWSN using AI focuses on energy efficiency monitoring for routing. An energy-efficient routing algorithm for SDWSN where control nodes are given different dynamic tasks is proposed. They utilised non-linear weight particle swarm optimization algorithm to create a cluster structure so to minimize the transmission distance to optimize the energy consumption of the network [19]. An energy-efficient monitoring algorithm in SDWSN using RL algorithm is proposed. The RL algorithm is designed in such a way as to perform value-redundancy filtering and load-balancing routing per the values and distribution of flows, respectively to improve the energy efficiency self-adaptability to environmental change of WSNs.

The proposed algorithm performs energy efficient routing by monitoring data flows and keeping track of each flow, this enables the network to handle request connection better. By keeping track of each flow, if another packet with the same address as the previously sent packet is sent, the nodes can just forward the node without having to recalculate the route.

### B. *Energy-Efficient Monitoring Using Reinforcement Learning*

The mechanism that is based on RL is embedded in the control plane for information processing, where the interaction between agents and the environments are utilised to enhance the intelligence in policy making to improve the self-adaptability of the energy-saving mechanism [30]. This algorithm guarantees improved QoS by mining the application specific value distribution and redundancy of data flows. This is supposed to consider the constraints of WSNs which are specified in terms of radio sources, energy and computational capabilities.

Based on the experimental results, the system prototype can improve energy efficiency by effectively inhibiting the transmission of value-redundant loads, reducing the amount of cross-plane communications and enhancing the load balance in SDWSN. The proposed system does provide good energy mechanism but lacks when it comes to scalability of the control plane.

### C. *Security in SDWSN*

Security is a serious issue, intruders are always looking for new ways to infiltrate networks. We have internal (try to raise their access privileges to misuse non-authorised privileges) and external intruders (targets network trying to gain unauthorised access to system information). There are different kinds of IDS which are active and passive IDS, Network intrusion detection systems (NIDS) and Host intrusion detection systems (HIDS), knowledge-based (ignature-based) IDS and behaviour-based (anomaly-based) IDS. This IDS mentioned have drawback when used traditionally, passive IDS are not capable of performing any protection or corrective functions on its own.

HIDS find it difficult to analyses the intrusion attempts on multiple computers, find it difficult to maintain large network with different operating systems and configuration. Knowledge-based IDS needs a continuous update and to be maintained, they fail to identify unique attacks. Behaviour-based IDS have high false alarms. With these drawbacks, we

attempt to introduce machine learning algorithms which try to solve this issue, this will introduce intelligent IDS.

WSN suffers major resource constraints when coming to implementing optimal security measures, with SDN being applied to WSN this opens new possibility but with these possibilities brings more risk. Applying AI techniques in SDWSN will mitigate this risk to an acceptable level. One of the techniques done is called a hybrid IDS where knowledge- and behaviour-based IDS are combined. Using machine learning technique in a hybrid IDS brings new capabilities, decrease in false alarms in anomaly detection, decrease in new threats signature updates. The hybrid IDS will allow the IDS to have a better chance in detecting unique attacks.

## VI. Summary and Discussion

QAR research provides solution to signalling delays and QoS-aware adaptive routing and another research introduced a framework that provides QoS traffic classification in routers refer to Table I below. Machine learning techniques applied to this research aims to monitor traffic in the network and improve the routing capabilities of the network which can reduce delay time, flooding of packets in the network. They both have transportation of packet to different nodes or stations as a common factor. Packets should be routed efficiently and needs to be monitored so that the routers are not flooded with packets from different nodes.

Networks need to have a fast response time when it comes to packets being transported that is the ability for fast connection, application of this techniques to SDWSN will surely improve routing capability of the network but like all techniques, challenges will be experienced but may be limited and the techniques may be improved with further research.

Supervised and semi-supervised algorithms appear to work wonders when it comes to network security using machine learning techniques, with the application of SDN to WSN to create SDWSN there comes a need for efficient and reliable network security, and with machine learning techniques applied to the network not only can the network be secured but the network can be able to learn patterns that future network attacks and threats have similar to old attacks, this will enable the network to adapt to this new threats based on what it has learned from previous attack and come up with an appropriate defence mechanism against this attacks. Machine learning techniques can also assist the network with an improved response time when it comes to this attacks since security measures deployed will be monitoring the flow of data in the network. Work done in [27], [28] are similar in a way that they focus on monitoring and detecting network threats, with this algorithm applied to SDWSN the security challenges from WSN can be improved with the network given an intelligent security and by combining algorithms in [25], [26] for QoS-aware and traffic monitoring security measurements in SDWSN will prove to be efficient, challenges might include training time of the network to efficiently monitor and prevent threats.

With the challenges experienced by WSN these techniques summarised in table 1 will provide suitable solutions. These techniques above bring a new approach to networks giving them the ability to maintain themselves when faced with problems. Security detection techniques discussed and summarised in table 1 will improve the security of SDWSN by providing the network with the ability to monitor traffic flow, categorise the flow and detect threats fast with fast response time. Possible challenges with the techniques applied to SDWSN comes when new application arrive and more data is required to be transported using the network, also security threats become smarter each day thus maintaining an algorithm capable of adapting to new security threats that arise might prove to be a challenge. Choosing the correct routing path in an instance may prove to be a challenge if the network is unable to perform multiple tasks at the same time, choosing the correct path, monitoring the path for corrupt data, ability to handle increase in traffic flow of data, etc.

TABLE I. Summary table

| Reference | Application | AI technique | Objective | Challenges |
|---|---|---|---|---|
| Chen-xiao *et al.* [23] | Routing | Back propagation neural network | real time dynamic load balance to decrease the latency | Energy efficinecy |
| Dobrijevic *et al.* [24] | Routing | Ant Colony Optimization | Improve QoE | Handling traffic |
| Kaur *et al.* [16] | Routing | QAR using Reinforcement Learning | Improve QoS | Difficulty handling real time traffic flow |
| Wang *et al.* [26] | Traffic classification | Laplacian SVM | Classifies data flows to efficiantly save energy | Difficult to keep track of all data especially with new devices connecting |
| Xiang *et al.* [19] | Routing | Particle swarm optimization | Energy- effcient routing | Requires a lot of control nodes for less energy to be used |
| Wang *el al.* [27] | Security | Improved behaviour based SVM | DDos detection | Difficulty in adapting to new data |
| Barki *el al.* [28] | Security | 1.Naïve bayes<br>2.K nearest neighbor<br>3.K means, 4.K medoids | DDoS and DoS attack detection | Difficulty handling large amount of data |
| Leguay *et al.* [29] | Admission Control | Cost-Sensitive | Connection request validation | Each day a bundle of connection request comes through and some are unable to be accepted |
| Huang *et al.* [30] | Energy-Effciency monitoring | Reinforcement Learning | To monitor energy efficiency | Difficulty maintining the network scalability |

## VII. Conclusion

Work on artificial intelligence focusing on improving routing and security capabilities in SDN are reviewed in this paper. AI brings intelligence to networks and with it applied to networks this brings reliable and secure networks with the capability to improve response time when it comes to detecting and solving attacks in networks and when it comes to reducing floods in networks. AI in SDWSN will bring intelligent network with the ability to self-calibrate, adapt to new condition and monitor flows in the network and can make decision without third party interference. Applying AI techniques shown in table 1 to SDWSN will bring merit to the network which is what is needed due to many applications being introduced each day, but we do expect challenges to occur thus more research can be taken to figure out what kind of improvement to the techniques discussed should be implemented to provide efficient routing, security or energy efficient monitoring to the network for required QoS and QoE.

## References


[1] A. M. Abu-Mahfouz, T. Olwal, A. Kurien, J. L. Munda, and K. Djouani, "Toward developing a distributed autonomous energy management system (DAEMS)," in *Proc. of the IEEE AFRICON 2015 Conference on Green Innovation for African Renaissancce*, 2015, pp. 1–6.

[2] P. Dongbaare, S. P. Chowdhury, T. O. Olwal, and A. M. Abu-Mahfouz, "Smart Energy Management System based on an Automated Distributed Load Limiting Mechanism and Multi-Power Switching Technique," in *Proceedings of the 51st International Universities' Power Engineering Conference*, 2016.

[3] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," in *Proc. of the IEEE International Conference on Industrial Informatics*, 2015, pp. 993–998.

[4] A. M. Abu-Mahfouz, Y. Hamam, P. R. Page, and K. Djouani, "Real-time dynamic hydraulic model for potable water loss reduction," *Procedia Eng.*, vol. 154, no. 7, pp. 99–106, 2016.

[5] B. Cheng, L. Cui, W. Jia, W. Zhao, and P. H. Gerhard, "Multiple Region of Interest Coverage in Camera Sensor Networks for Tele-Intensive Care Units," *IEEE Trans. Ind. Informatics*, vol. 12, no. 6, pp. 2331–2341, Dec. 2016.

[6] B. Silva, R. M. Fisher, A. Kumar, and G. P. Hancke, "Experimental Link Quality Characterization of Wireless Sensor Networks for Underground Monitoring," *IEEE Trans. Ind. Informatics*, vol. 11, no. 5, pp. 1099–1110, Oct. 2015.

[7] K. S. E. Phala, A. Kumar, and G. P. Hancke, "Air Quality Monitoring System Based on ISO/IEC/IEEE 21451 Standards," *IEEE Sens. J.*, vol. 16, no. 12, pp. 5037–5045, Jun. 2016.

[8] A. M. Abu-Mahfouz and G. P. Hancke, "Evaluating ALWadHA for providing secure localisation for wireless sensor networks," in *IEEE AFRICON Conference*, 2013, pp. 501–505.

[9] N. Ntuli and A. M. Abu-Mahfouz, "A Simple Security Architecture for Smart Water Management System," *Procedia Comput. Sci.*, vol. 83, no. 4, pp. 1164–1169, 2016.

[10] J. Louw, G. Niezen, T. D. Ramotsoela, and A. M. Abu-Mahfouz, "A key distribution scheme using elliptic curve cryptography in wireless sensor networks," in *Proceedings of the 14th IEEE International Conference on Industrial Informatics*, 2016, pp. 1166–1170.

[11] A. M. Abu-Mahfouz and G. P. Hancke, "ALWadHA Localisation Algorithm: Yet More Energy Efficient," *IEEE Access*, vol. 5, no. 5, pp. 6661-6667, 2017.

[12] A. M. Abu-Mahfouz and G. P. Hancke, "Localised Information Fusion Techniques for Location Discovery in Wireless Sensor Networks," *Int. J. Sens. Networks*, 2017.

[13] B. Silva and G. P. Hancke, "IR-UWB-Based Non-Line-of-Sight Identification in Harsh Environments: Principles and Challenges," *IEEE Trans. Ind. Informatics*, vol. 12, no. 3, pp. 1188–1195, Jun. 2016.

[14] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke, "Using Cognitive Radio for Interference-Resistant Industrial Wireless Sensor Networks: An Overview," *IEEE Trans. Ind. Informatics*, vol. 11, no. 6, pp. 1466–1481, Dec. 2015.

[15] S. Lin, P. Wang, and M. Luo, "Jointly optimized QoS-aware virtualization and routing in software defined networks," *Comput. Networks*, vol. 96, no. 2, pp. 69–78, 2016.

[16] H. Kaur and S. Sahore, "A survey on wireless sensor network (wsn) security using AI methods," *Int. J. Latest Trends Eng. Technol.*, vol. 7, no. 4, pp. 234–239, 2016.

[17] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements," *IEEE Access*, vol. 5, no. 1, pp. 1872–1899, 2017.

[18] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software Defined Wireless Sensor Networks Application Opportunities for Efficient Network Management: A Survey," *Comput. Electr. Eng.*, 2017.

[19] W. Xiang, N. Wang, and Y. Zhou, "An Energy-Efficient Routing Algorithm for Software-Defined Wireless Sensor Networks," *IEEE Sens. J.*, vol. 16, no. 20, pp. 7393–7400, Oct. 2016.

[20] M. Ndiaye, G. P. Hancke, and A. M. Abu-Mahfouz, "Software Defined Networking for Improved Wireless Sensor Network Management : A Survey," *Sensors*, vol. 17, no. 5: 1031, pp. 1–32, 2017.

[21] M. Latah and L. Toker, "Application of Artificial Intelligence to Software Defined Networking: A Survey," *Indian J. Sci. Technol.*, vol. 9, no. 44, pp. 1–7, 2016.

[22] H. Bai, "A survey on artificial intelligence for network routing problems," *Univ. New Mex.*, pp. 1–10, 2007.

[23] C. Chen-xiao and X. Ya-bin, "Research on Load Balance Method in SDN," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 1, pp. 25–36, 2016.

[24] O. Dobrijevic, M. Santl, and M. Matijasevic, "Ant Colony Optimization for QoE-Centric Flow Routing in Software-Defined Networks," *11th Int. Conf. Netw. Serv. Manag.*, pp. 274–8, 2015.

[25] S. Lin, I. Akyildiz, and P. Wang, "QoS-aware adaptive routing in multi-layer hierarchical software defined networks: a reinforcement learning approach," in *IEEE International Conference on Services Computing*, 2016, pp. 25–33.

[26] P. Wang, S. Lin, and M. Luo, "A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs," in *IEEE International Conference on Services Computing*, 2016, pp. 760–765.

[27] P. Wang, K. Chao, H. Lin, and W. Lin, "An Efficient Flow Control Approach for SDN-Based Network Threat Detection and Migration Using Support Vector Machine," in *IEEE 13th International Conference on e-Business Engineering*, 2016, pp. 56–63.

[28] L. Barki, A. Shidling, and N. Meti, "Detection of distributed denial of service attacks in software defined networks," in *IEEE International Conference on Advances in Computing, Communications and Informatics*, 2016, pp. 2576–2581.

[29] J. Leguay, L. Maggi, M. Draief, S. Paris, and S. Chouvardas, "Admission Control with Online Algorithms in SDN," no. Noms, pp. 718–721, 2016.

[30] R. Huang, X. Chu, J. Zhang, and Y. H. Hu, "Energy-Efficient Monitoring in Software Defined Wireless Sensor Networks Using Reinforcement Learning: A Prototype," *Int. J. Distrib. Sens. Networks*, vol. 11, no. 10, pp. 1–12, 2015.