Analysis of Notable Security Issues in SDWSN

Mbongeni Manuel
Department of Computer Science
North-West University
Mafikeng, South Africa
mbongenimanuel@gmail.com

Bassey Isong
Department of Computer Science
North-West University
Mafikeng, South Africa
isong.bassey@ieee.org

Michael Esiefarienrhe
Department of Computer Science
North-West University
Mafikeng, South Africa
michael.esiefarienrhe@nwu.ac.za

Adnan M. Abu-Mahfouz
Modelling and Digital Science
CSIR
Pretoria, South Africa
a.abumahfouz@ieee.org

***Abstract*—Wireless Sensor Networks (WSNs) are network paradigm that are constrained by several challenges such as management of the network, energy consumption, data processing, quality of services (QoS) provisioning, and security. Software-Defined Networking (SDN) emerged as a viable solution to mitigate these inherent challenges yielding SDWSN. SDWSN is gaining momentum and has brought innovation, ease of network management and configuration through network programmability. However, SDWSN is not immune to challenges due to several issues inherited from both the WSN and SDN. Although several research works have been carried out aimed at proffering solutions, there is still more to be done to ensure SDWSN is secure, dependable, and scalable. Therefore, this paper brings together some of the notable issues that needs to be addressed and some of the solutions already proposed or developed. The objective is to get insights into these challenges and provide some solutions. We presented and discussed specifically, the security issues with respect to SDWSN model, threats, attacks, and some of the existing countermeasures.**

Keywords*— *WSN, SDWSN, security attacks, challenges.

I. Introduction

Wireless Sensor Network (WSN) comprises of small sensor equipped with capability of checking physical and natural variables, like temperature, humidity, vibrations, movements, seismic occasions, and so on [1, 2]. Sharma *et al.* [3] defined a sensor node as that which gathers information about physical and natural variables from fields, process and propagates the processed information with other nodes in the network. This network paradigm has created great impacts on Internet of Things (IoT) and cloud computing, since the sensing nodes are the most building blocks of this concept [3, 4]. WSNs stand as one of the foremost developing advances combining together sensing, computational capability and communication into miniature devices continuing towards entirety modern world of simplicity. In the perspective of IoT, [5] predicted that about 50 billion devices will be connected to the Internet by the year 2020 where most of these devices will be equipped with sensors and actuators. The technology of WSNs is utilized to close the gap between the physical and computer-generated world of electronic gadgets like computers [6]. Its significance lies in its widespread application due to their cost-effective characteristics such as in the military, restorative, and different keen frameworks for instance Smart City, Smart Grid and Smart Water Framework [7 - 9]. However, WSN is faced with several challenges related to the asset confinement of the sensor equipment to be specific, processing, memory, energy and communication capabilities, in spite of the fact that they are broadly utilized because of the expanded amount of inserted devices accessible for simpler sending [10]. Other issues are quality of service (QoS), scalability and reliability [11 - 14]. These issues are inherent to sensor networks because the nodes are made to have functionalities from the physical layer to the application layer carrying on to be an independent system that forwards data and manages the network [15]. Although, it operates correctly, it still needs effortlessness and adaptability which will make it difficult to oversee whenever attempting to execute a long range and low power WSN at a large-scale [10]. Due to these inherited challenges, securing WSN is not a trivial task [38, 39].

Software-defined networking (SDN) is an architecture for computer networking that gives a clear partition between network control capacities and forwarding operations. This architecture aimed to simplify the usage of a few tasks that are critical to network operation, such as routing and network administration [14]. SDN has gained momentum recently and attracted application in several areas because it works on a design leading to the partitioning of the data plane and control plane through the OpenFlow interface [15]. The most important aspect of the SDN model is that it is designed to address majority of the issues plaguing WSNs, particularly energy consumption, which could be the cause of the network life expectancy and performance. However, majority of the energy severe capacities are delegated to the centralized node from the physical node. These nodes become devices that cannot perform routing, processing, and management functions but performed by the controller [15]. The incorporation of SDN into WSN has yielded to a modern paradigm called Software Defined Wireless Sensor Network (SDWSN). Thus, SDWSN provides the following benefits to the WSNs:

- Energy saving: WSN nodes are energy-constrained, leading to the limitations in the design and implementation of sensor application and network protocol. Therefore, SDN promises an energy-efficient way for sensor network management.
- Sensor node mobility: The structure of the mobile sensor network changes frequently depending on the degree of mobility. If centralized SDN controller manages mobility routing decisions and policies could be modified at sensor nodes which could lead to lower convergence time.

TABLE I. SECURITY THREATS IN DIFFERENT LAYERS OF SDN [18]

Security threats	**Security strategies**	**Security requirements**	**Affected functionalities**	**Application layer**	**Control layer**	**Northbound “NI”or Southbound interface “SI”**	**Data layer**
Operating system alteration	Trusted computing	System integrity protection	Application management	✓	✓		✓
Software framework alteration	Trusted computing	System integrity protection	Application management	✓	✓		✓
Software failure	High assurance	Robustness, system integrity protection	All functionalities	✓	✓		✓
Hardware failure	High assurance	Robustness, system integrity protection	All functionalities		✓		✓
Configuration data alteration	Data integrity functionality in SDN middleware	Data integrity protection	Resource management, application management		✓	SI	✓
Configuration data extraction	Data integrity functionality in SDN	Confidentiality protection	Data management		✓	SI	✓
Unauthorized access to SDN services	Deploying secure administration module	Identities verification, ensuring system integrity	All functionalities	✓	✓	NI and SI	✓
User data alteration	Data integrity functionality in SDN	Ensuring data integrity	Data management				✓
Masquerading as authorized SDN controller	Use of digital signatures for SDN software	Ensuring system integrity, identities verification, accountability	Application management		✓	SI	✓

- Network management: Network management is one of the complex aspects in WSNs, hence SDNs promises a neat and flexible solution to management problems in WSNs.
- Localization accuracy and topology discovery: In many sensor networks localization is very important, because of the sensor nodes’ energy-constrained nature it is therefore important to achieve highly-accurate location information with the help centralized location algorithm. With the utilization of SDN the gathered location information can be combined at the centralized controller where it can be used by a network topology discovery algorithm to enhance routing decision made by the controller.

Despite the benefits of SDWSN in the realm of WSN, several challenges still exist. Many of the identified issues are as a results of resource limitation of WSNs [16] and those inherited from SDN. Moreover, the advancement of the SDWSN architecture is still in its earliest stages but profitable advances have been made within the research communities. In spite of the distinctive applications of the architectures, they all adjust to the basics of SDN. Therefore, this paper brings together some of the notable issues and currently available countermeasures of SDWSN challenges. The objective is to gain insights into these issues and make them available to researchers in order channel research activities aim at ensuring a more secure, dependable and scalable SDWSN networking paradigm.

The remaining parts of the paper are organized as follows: Section II presents the related works in SDWSN. Section III highlights and discusses the security issue in the SDWSN. In Section V discusses the findings, Section VI presents the paper conclusion.

II. RELATED WORKS

There are several existing review and survey works on the issues of SDN-SDWSN. Some of the studies are discussed as follows: Kgogo *et al.* [15], presented numerous issue of security in SDWSN coming from the view of WSN and SDN and some of the solutions that addressed such challenges. The study outlined security issues faced by SDWSN and concluded that the network paradigm is in its early stages and security aspects of the networks still need to be addressed. They also provided suggested ways to mitigate attacks within the SDWSN which is also applicable to the entire network [15]. Pritchard *et al.* [17] emphasized security as one of the foremost vital facet of any network which has been neglected in the improvement of SDWSN. They analysed the security problems with SDN and WSN individually as there is a need to consolidate SDN and WSN security methods to address the challenges of SDWSN alone. WSNs have several inherent problems like unavailability of resources resulting in the failure to apply security measures in its initial architectural design. SDN has its difficulties like trade-off amongst functionality and performance particularly on the forwarding plane [17].

In a similar study, Kobo *et al.* [16] studied the recent modern application of SDN in WSNs which falls within the larger context of IoT. They presented the bottom-up approach within SDN application to the realisation of IoT and explored the impact of having SDWSN. The problems of SDWSN paradigm for instance energy, network management, configuration, scalability, routing, mobility, localization interoperability, communication and security are predicted to progress [16]. They also presented the challenges surrounding future of SDWSN and identified important design requirements. The conclusion is that not much work has been done on SDWSN challenges since it is a networking model that has just been developed. Furthermore, Akhunzada *et al.* [18] from SDN point of view defined few of the security issues originating from the control plane.

In some of the review papers highlighted above, several notable issues were not discussed. All these papers have to be read before comprehending the important challenges that exist. Thus, this paper fills the gap by bringing together these issues faced by SDWSN. As SDWSN model is advancing, attackers are developing new techniques to harm the network either through the planes or the periphery devices. Hence, it is important to secure it against all threats and attacks.

III. Security Issues in SDN-SDWSN

This section highlights some of the challenges faced in SDWSN. They are discussed as follows:

Shaghaghi *et al.* [19], identified the challenges confronted with securing the data plane of SDN which is one of the least investigated but most critical component of this technology. They highlighted the critical role of data plane in the implementation of network policies with the need to ensure that it is secured and protect from attackers. This is because compromising forwarding devices can potentially take down an entire SDN system. They stated that existing solutions suffered from limitations that hindered their real-world applications. Thus, a more advance and practical protecting mechanism is needed. There is also the need to evaluate the applicability of existing solution for effective forwarding devices and designing a secure hardware for SDN-enable forwarding devices based on the latest software advances and requirements. Moreover, [19] presented a taxonomy of attacks against SDNs based on their scope and impacts. Particularly, discussing how an adversary can use vulnerabilities of distinctive SDN components to target network policies, their enforcement, and implementation. They also stated the importance of securing the SDN data planes and establish a set of suggestions for a working solution as well as reviewed the existing solutions with regard to these requirements.

Pritchard *et al.* [17] stated that there is a need to adapt the existing solutions to study the SDWSN alone. They identified that proposed solutions must be evaluated to ensure their validity and the control plane must be protected from attacks. One of such validation is to ensure whether for instance, sensor nodes poses a threat to the data plane or not [17]. Moreover, they stated that though SDN approach is beneficial, they also introduced new threats and attacks that could harm and compromise the entire networks. Some of the threats discussed in [17] are:

- Application plane: Issues are centred on authentication and authorization in terms of network attacks [20]. This is as a result of no existing techniques for certification and the management of trust.
- Controller plane: The issues is that the control plane is the potential target of attacks due to its criticality. Thus, attacks such denial of service (DoS) attacks and data theft can results in the failure of the entire networks.
- Data plane: Fake traffic flows, assaulting vulnerabilities in switches are the threats of the data plane due to misconfiguration of the devices and attacker [20]. A malicious user can infuse fake flows into the network once the control of the server has been gained.

In addition, [17], suggested effective security measures for the SDN ranging from the detection of threats, remediation to the correctness of the network as well as the security as a service. Most researchers concurred to the suggestion that security should be considered when designing SDNs. Accordingly, Ahmad *et al.* [20] proposed several approaches to incorporate security into the control plane. They include: the prevention of attacks such as DoS and DDoS ensuring security through reliable controller placement, protecting against application that are malicious or faulty and protecting against attacks that impacts the control plane' scalability effort.

Chen *et al.* [21] also identified other security challenges that affects the SDN which include attacks on the controller and switches vulnerabilities, forged flow of traffic, control plane communication attacks and the management of trust between applications and controller. Consequently, the network needs to be aware and mindful of any potential threat which should be addressed during its design. Within the perspective of SDN, Ali *et al.* [22] explained that, SDN security can be improved by incorporating the security features into its architecture. To this effect, Han and Ren [23] proposed a cluster-based routing protocol in an OpenFlow-based SDN using three types of nodes: master node, centre node, and a normal node. The master node serves as the controller, the centre node is the switch/sensor while the normal node accepts data. Moreover, SDN-based virtualization application model FlowVisor [24, 25] was used to enables multiple controllers to utilize or manage one switch simultaneously. Akhunzada *et al.* [18] also presented several important security threats that negatively affects the different layers of the SDN paradigm. Summary of these threats are captured in Table I. They include the different threats, their strategies, the security requirements needed, the impacted functionalities and the different layer affected.

Modieginyane *et al.* [26] also recognized that security is a major concern in the SDN. Their work reported that security is still an issues because of the following questions that still ascend:

- What method will be used to implement security in the SDN infrastructure?
- If security is implemented in SDN centralized controller, what will happen when the controller is compromised with attacks?

- Should there be a few level of security in each portion of the SDN design?

In addition, Modieginyane *et al.* [26], considered challenges that are presently emanates from both SDN and SDWSN approaches, being referred to as whether they could enhance general WSN applications. They encouraged on network basic perspectives, such as security, reliability and scalability, since these are probably the most central points that should be considered when wanting to enhance or streamline network functionalities. Vigorous types of framework testing could be utilized to abuse the system of any security weakness, in light of the fact that the endeavour of growing intense security for SDWSN is a continuous process [26]. The utilization of centralized controller in SDWSN brings up some security questions that show up with the introduction of SDNs such as [27]:

- What might be the impact if assaults are coordinated towards the controller?
- What might be the impact of a vindictive controller on the system?

Dhamecha and Trivedi [28], examined security issues and challenges in SDN and the current state-of-the-art. They further, stated that SDN is still developing, hence such a significant number of challenges emerge while conveying it in current networks. They concluded by expressing that there should be different security applications and extra security layer on top of the physical layer to ensure the security of the controller [28]. Ali *et al.* [22], expressed that security has assumed critical significance lately due to a number of reasons, hence they directed a survey of security issues of SDN by analysing basic undertakings of securing the SDN. In addition, featuring that there is an earnest requirement for security component which deciphers security privileges over domain restrictions. They categorized SDN-based security research in two branches: (1) research equipped towards ensuring the protection of the network, and (2) providing Security as a Service (SaaS).

Kreutz *et al.* [29], expressed the need to join security and trustworthiness into SDN from the early stages. Taking note of the fact that dangers in SDN are not just of an alternate nature when contrasted with traditional networks. They layout certain classes of security threats which might be utilized to assault SDN such as forged traffic flows, DoS attacks, etc. Moreover, the research efforts to mitigate these challenges are steps in the right direction, however there is an enormous measure of work to be done before SDN can be certainly sent in the real world because we can no longer bear the cost of a receptive security methodology that the business took with traditional networks [19].

Moreover, Jacobsson and Orfanidis [30] detailed that the SDN approach for WSNs is confronted with issues due to the resource constraint and management. Nunes *et al.* [31] further added that challenges of efficient utilization of resources particularly in wireless multi-hop ad-hoc network is due to the inherent limitation of the wireless capacity. [30] Went further to proposed the design of an architecture that is adaptable for WSN and IoT that are based on SDN and where in-network processing is considered an integral part. They also proposed to validate the architecture by implementing a prototype, ensure communication between control plane and the data plane and ensure energy efficiency in the SDWSN architecture. Also, the challenges of WSN devices and their capabilities as well as difference requirements stemming from the application scenarios are addressed by the SDWSN design [32]. Anadiotis *et al.* [33] proposed SDN solution which extends the approach of WSN called SD-WISE. The solution allows the wireless sensor nodes operating system to support the network function virtualization (NFV). In this case, SD-WISE exploits ensure that sensor nodes will carry on as imposed by a remote recognized authority on the basis of the current context.

IV. Discussions

SDN is a network technology that has gained considerable momentum today and has brought innovation, ease of management and configuration to the networks through programmability technique. However, it is also face with several challenges. This paper reviewed the challenges faced with the SDN approach and the newly developed network paradigm, SDWSN. It presented several proposed and developed solutions that can be used to mitigate some of the challenges of SDWSN. The review found that SDWSN is faced with several security challenges inherited from the SDN and the WSN. Moreover, the network technology is still in its early stage. Though several research have been performed in the perspectives of SDN and WSN separately, there are no enough work done on SDWSN alone. Table II presents a summary of some of the challenges identified, some solutions proposed and tools/techniques used. It also presents a summary of the future work presented by each researcher in the area of SDWSN. In addition, we found that the choice of tools in the implementation of SDWSN is very important. Some of these tools are shown in TABLE II. For instance, "Mininet" supports collaborative network research in terms of flexibility, deployment, interaction, scalability, realization and sharing [32]. W3 supports troubleshoot bugs in SDN control software [36]. Reitblatt *et al.* [37] developed a declarative language "FatTire" that supports fault-tolerance requirements and provide compiler with fast-failover mechanism. Moreover, FS-SDN by Gupta *et al.* [34] supports large scale networks compared Mininet.

Given the above challenges and some of the solutions as well as tools, we also found out that there is a gap in building effective security framework for the model and some of the proposed solution have not yet been validated. Thus, to ensure that SDWSN is secure, dependable and scalable, proactive security measures should be developed, validated and put in place.

V. Conclusion

This paper presented some of the security issues that confronts SDWSN and few of the proposed and developed countermeasures to address the challenges. We found that SDWSN is faced with several challenges emanating from SDN and WSN. Moreover, SDWSN is still new technology. However, SDWSN is gaining widespread applicability and several researchers within the industry and academia are the

TABLE II. Summary of Challenges and some Countermeasures in SDN-SDWSN

Ref.	Challenges	Solutions	Tools/ Techniques	Future work
[15]	There is a need to look at the security challenges of SDWSN alone SDWSN lacks Middle boxes, Transport layer security	Components to moderated security assaults in SDWSN has to be outlined and executed.		Security model framework should be planned to secure the whole network and the protocols utilized for communication inside the network.
[18]	Securing the control plane against all threats. Study should confirm whether sensor nodes utilized in SDWSN posture less of a threat to data plane. Data sending issues on the data plane ought to be settled. Adapting the solutions proposed to contemplate SDWSN alone.	Centralization of control to simplify network management resulting in less resource constraints on the node.	FlowChecker, VeriFlow.	Security challenges should addressed in order to realize secure SDWSNs, especially in the advancement of the IoT paradigm.
[19]	The need to ensure that SDN is secured and protect from attackers. Existing solution suffer from limitations (it is expected to propose more advance and practical protecting mechanism on the ground of existing limitations) Securing the data plane of SDN which is one of the least investigated but most critical component of this technology.	Presented a taxonomy of attacks against Software-Defined Networks based on their scope and impacts.	NOX-MT, Maestro, Beacon, Ryu NOS, Floodlight, ONOS, Onix, HyperFlow, PANE, DISCO.	Evaluate the applicability of existing solution for stateful forwarding devices and propose solutions to ensure if any such device is fully, partially, compromised it can be detected.
[28]	Network management Performance tuning Error-prone.	Solution that uses a map to collect all the topological information from the nodes called (SDWSN).	Mininet, Flowvisor, RouteFlow, NICE, Anteater, OFRewind, VeriFlow, and STS.	A viable technique to ensure efficient utilization of resources in future networks.
[33]	WSN devices and their capabilities as well as the large difference requirements stemming from the application scenarios are addressed by the SD-WISE design.	Proposed SD-WISE networking solution.	SD-WISE.	To ensure that sensor nodes will carry on as imposed by a remote recognized authority on the basis of the current context.
[37]	How to differentiate between threats and inconsistencies for completely programmable and repurposable network nodes, where whole conduct is not a priori known? The design of abstractions and platforms for programmable monitoring tasks.	Specifically highlighted possible vulnerabilities specific to stateful in-switch processing which should be taken into consideration in future directions.	Mininet	There are a few plans proposed, each of which tending to a particular require in bringing stateful SDN data plane into reality. However, none of them has built-in security measure.

major players. Though, several solutions have been proposed or developed, more solution ought to be developed to ensure the security and dependability of SDWSN. Given the different security issues identified, there is the need to channel research efforts and activities to address them in SDWSN. Thus, our future work will attempt to provide solutions to some of the identified security issues in the SDWSN.

Acknowledgment

This research was supported by FRC and the Department of Computer Science at the NWU-Mafikeng and CSIR, South Africa.

References

[1] G Abu-Mahfouz, A.M. and G.P. Hancke, Localised information fusion techniques for location discovery in wireless sensor networks. International Journal of Sensor Networks, 2018. 26(1): p. 12-25.

[2] Ogbodo, E.U., D. Dorrell, and A.M. Abu-Mahfouz, Cognitive Radio Based Sensor Network in Smart Grid: Architectures, Applications and Communication Technologies. IEEE Access, 2017. 5: p. 19084-19098.

[3] Sharma, A., *et al.*, A Survey Paper on Security Protocols of Wireless Sensor Networks. 2015, IJEIT.

[4] Akpakwu, G.A., *et al.*, A survey on 5G networks for the internet of things: communication technologies and challenges. IEEE Access, 2018. 6: p. 3619-3647.

[5] Computing, F., *the Internet of Things: Extend the Cloud to Where the Things Are.* Available on: http://www. cisco. com/c/dam/en_us/solutions/trends/iot/docs/computingoverview. pdf, 2015.

[6] Sharma, S., R.K. Bansal, and S. Bansal. Issues and challenges in wireless sensor networks. in Machine Intelligence and Research

Advancement (ICMIRA), 2013 International Conference on, pp. 58-62. IEEE (2013).

[7] T.D. Ramotsoela, A.M. Abu-Mahfouz and G.P. Hancke, “A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study,” *Sensors*, vol. 18, no. 8: 2491, pp. 1-24, 2018. Doi: https://doi.org/10.3390/s18082491

[8] Abu-Mahfouz, A.M., *et al. Toward developing a distributed autonomous energy management system (DAEMS)*. in *AFRICON, 2015*. 2015. IEEE.

[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] H.I. Kobo, A.M. Abu-Mahfouz, G.P. Hancke, “Fragmentation-based Distributed Control System for Software Defined Wireless Sensor Networks,” IEEE transactions on industrial informatics, in press, 2018. DOI: 10.1109/TII.2018.2821129

[11] Cheng, B., *et al.*, Multiple region of interest coverage in camera sensor networks for tele-intensive care units. IEEE Transactions on Industrial Informatics, 2016. 12(6): p. 2331-2341.

[12] Kumar, A. and G.P. Hancke, *A zigbee-based animal health monitoring system.* IEEE sensors Journal, 2015. 15(1): p. 610-617.

[13] Phala, K.S.E., A. Kumar, and G.P. Hancke, *Air quality monitoring system based on ISO/IEC/IEEE 21451 standards.* IEEE Sensors Journal, 2016. 16(12): p. 5037-5045.

[14] da Silva, A.S., *et al.*, *Resilience support in software-defined networking: A survey.* Computer Networks, 2015. 92: p. 189-207.

[15] Kgogo, T., B. Isong, and A.M. Abu-Mahfouz. Software defined wireless sensor networks security challenges. in AFRICON, 2017 IEEE. 2017. IEEE.

[16] Kobo, H.I., A.M. Abu-Mahfouz, and G.P. Hancke, *A survey on software-defined wireless sensor networks: Challenges and design requirements.* IEEE Access, 2017, vol. 5, no. 1, pp. 1872-1899, 2017.

[17] Pritchard, S.W., G.P. Hancke, and A.M. Abu-Mahfouz. Security in Software-Defined Wireless Sensor Networks: Threats, Challenges and Potential Solutions. in IEEE Int. Conf. of Ind. Informat., Emden, Germany. 2017.

[18] Akhunzada, A., *et al.*, *Secure and dependable software defined networks.* Journal of Network and Computer Applications, 2016. 61: p. 199-221.

[19] Shaghaghi, A., *et al.*, Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions. arXiv preprint arXiv:1804.00262, 2018.

[20] Ahmad, I., *et al.*, *Security in software defined networks: A survey.* IEEE Communications Surveys & Tutorials, 2015. 17(4): p. 2317-2346.

[21] Chen, J., X. Zheng, and C. Rong. Survey on software-defined networking. in International Conference on Cloud Computing and Big Data in Asia. 2015. Springer.

[22] Ali, S.T., *et al.*, *A survey of securing networks using software defined networking.* IEEE transactions on reliability, 2015. 64(3): p. 1086-1097.

[23] Han, Z.-j. and W. Ren, *A novel wireless sensor networks structure based on the SDN.* International Journal of Distributed Sensor Networks, 2014. 10(3): p. 874047.

[24] Sayyed, R., *et al.* Resource optimization using software defined networking for smart grid wireless sensor network. in Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference on. 2014. IEEE.

[25] Sherwood, R., *et al.*, *Flowvisor: A network virtualization layer.* OpenFlow Switch Consortium, Tech. Rep, 2009. 1: p. 132.

[26] 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. Elect. Eng., no. 3, pp. 1–14, 2017.

[27] A. De Gante, M. Aslan, and A. Matrawy, ‘‘Smart wireless sensor network management based on software-defined networking,’’ in Proc. 27th Biennial Symp. Commun., Jun. 2014, pp. 71–75.

[28] Dhamecha, K. and B. Trivedi, Sdn issues-a survey. International Journal of Computer Applications, 2013. 73(18).

[29] Kreutz, D., F. Ramos, and P. Verissimo. Towards secure and dependable software-defined networks. in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013. ACM.

[30] Jacobsson, M. and C. Orfanidis. Using software-defined networking principles for wireless sensor networks. in 11th Swedish National Computer Networking Workshop (SNCNW 2015) Karlstad, May 28-29, 2015. 2015.

[31] Nunes, B.A.A., *et al.*, A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 2014. 16(3): p. 1617-1634.

[32] Lantz, B., B. Heller, and N. McKeown. *A network in a laptop: rapid prototyping for software-defined networks*. in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. 2010. ACM.

[33] Anadiotis, A.-C.G., *et al.*, *SD-WISE: A Software-Defined WIreless SEnsor network.* arXiv preprint arXiv:1710.09147, 2017.

[34] Gupta, M., J. Sommers, and P. Barford. Fast, accurate simulation for SDN prototyping. in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013. ACM.

[35] Dargahi, T., *et al.*, *A survey on the security of stateful SDN data planes.* IEEE Communications Surveys & Tutorials, 2017. 19(3): p. 1701-1725

[36] Scott, R.C., *et al.*, *What, where, and when: Software fault localization for sdn.* EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2012-178, 2012.

[37] Reitblatt, M., *et al. Fattire: Declarative fault tolerance for software-defined networks.* in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. 2013. ACM.

[38] 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 IEEE 14th International Conference on Industrial Informatics*, 18-21 July, Futuroscope-Poitiers, France, 2016. pp. 1166–1170.

[39] A.M. Abu-Mahfouz and G.P. Hancke, "Evaluating ALWadHA for providing secure localisation for wireless sensor networks," in *Proceeding of the IEEE AFRICON 2013 conference*, 9-12 September, Mauritius, 2013, pp. 501-505.