Software Defined Wireless Sensor Networks Security Challenges

Tebogo Kgogo, Bassey Isong
Computer Science Department
North-West University,
Mafikeng, South Africa
kgogot@gmail.com, isong.bassey@ieee.org

Adnan M. Abu-Mahfouz
Meraka Institute
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
a.abumahfouz@ieee.org

Abstract— **Wireless Sensors Networks (WSNs) have been gaining significant attention in both the industries and the academia in recent years. However, WSN are vulnerable to growing security threats and attacks which are inept for the current traditional security mechanisms to cope with or mitigate such security challenges. As a solution, Software Defined Network (SDN) has emerged and been merged with WSN to form what is known as Software Defined Wireless Sensor Network (SDWSN). SDWSN is introduced to bring flexibility, programmability and innovation to the WSN network. However, SDWSN is not exempted from security challenges. SDWSN is faced with multitude of security challenges inherited from both SDN and WSN which have become a bottle-neck to its operations and applicability. Therefore, this paper presents security challenges in both WSN and SDN which are transferable to SDWSN. We discussed the inheritable security challenges from the perspective of SDN and WSN by outlining several possible threats, attacks and some countermeasures. This is important to bring together these challenges in order to attract or stimulate more research and development activities aim at realizing a more secure and dependable SDWSN.**

Keywords— WSN, SDN, SDWSN, Security, Sensors

I. Introduction

The development of smart sensors in recent years has become the leading driving force of the advancements in wireless sensor networks (WSNs). WSNs are made of micro-sensors which are capable of monitoring physical and environmental factors like temperature, humidity, vibrations, motions, seismic events, etc. The wireless connection of WSNs allows the development of ad hoc networks without having to establish physical infrastructure or central management beforehand. In general, the knowledge of nodes position makes it easy to increase more useful and essential functions such as the specific area sensing as well as the improvement of network efficiency [1], [2]. Thus, the localization of node constitutes a key component for several WSNs applications [3], [4]. WSN as a network technology is used to ease the space between the physical world of human and the virtual world of electronic devices like computers [5]. Its importance lies on the fact that they have a lot of potential to proffer cost-effective solutions for problems such as in the military, medical, and various smart systems such as Smart City, Smart Grid and Smart Water System [6]–[8]. Furthermore, the introduction and proliferation of technologies like the Internet of Things (IoT) and others has skyrocketed the demand of WSNs as well as research and development activities in the field of WSNs in recent years.

Software Defined Network (SDN) is a network paradigm developed to cope with the inherent limitations and the lack of flexibility faced by the current traditional network management [9]–[11]. SDN is a network technology where network management is made easier and allows it to be dynamically controlled, changed and behavior managed through a technique called network programmability [9], [12]. The developmental goals of SDN were to simplify innovation and the programmability of the network management and control. In particular, SDN operates with the architecture that separates network control from its forwarding. It operates on an architecture that brings the separation of data and control plane through an interface called the OpenFlow. In recent years, SDN is gaining momentum and has attained widespread applications.

In the realm of computer networks, when SDN paradigm incorporates WSN, it manifest to a new network paradigm called Software Defined Wireless Sensor Network (SDWSN). SDWSN is today a new emerging paradigm for Low-Rate Wireless Personal Area Networks (LR-WPAN) [13]. It constitute one of the best approaches that can be used to improve the efficiency, sustainability of WSNs, foster interoperability with other networks as well as play a critical role in the looming IoT [14]. Considering the important application of WSNs, it is vital that WSN is secured and dependable. However, integrating full security in WSN constitute a challenging task when compared security in other networks. This is because there are several restrictions and constraints emanating from the fact that sensor nodes have limited processing power, energy, and storage as well as limited bandwidth in wireless links which are prone to failure. Moreover, sensors are prone to several cyber and physical attacks such as falsification of data, denial of service (DoS), interception of communication and so on [15]. However, these attacks are not different from attacks that are common to ad hoc networks on the basis that sensor nodes are neglected. Nonetheless, regardless of these challenges, security remains important and vital for many of sensor networks [15]. The integration of SDN with WSN will proffer an enhanced view of the SDWSN paradigm. In addition, SDWSN is not exempted from security challenges and has limited its operations and adoption. As a new paradigm, lots of work have not yet been done and it is important that these challenges are made known for research efforts to be channeled to them.

Therefore, in this paper we discuss the security challenges of both WSN and SDN and how these challenges affects the paradigm of SDWSN. The objective is to ensure that these challenges are made known to both current and future researchers in order to design and develop a secure and dependable SDWSN.

The remaining parts of the paper are organized as follows: Section II discussed security in WSN, Section III discussed on SDN security, Section IV outlined security in the SDWSN and Section V is paper conclusion.

II. Wireless Sensor Networks Security

In the realm of WSNs like other networks, WSNs are vulnerable to security threats and are associated with many security challenges [16]–[18]. In this section, we present some of the security threats that affect WSNs. One of such threats is known as spoofing. This threats has the capability to change network routing information, collect passive information, subvert nodes and perform several attacks such as sinkhole, Sybil, DoS and jamming [5], just to mention a few. However, data authentication, data confidentiality, data integrity, availability and redundancy are very important security requirement of WSN that still need to be ensured in any WSN system or application.

In particular, security has become a challenging problem in WSN because of its widespread applicability including battlefield, surveillance, building monitoring and in critical systems such as airports and hospitals [5]. To ensure that information transmitted between sensor nodes or between sensor nodes and base stations (BS) are in protective state, the security goal of confidentially is indispensable. This is vital to avoid the communications being eavesdropped by attackers [5]. With WSN, it is very important for sensor nodes and BS to be equipped with the capability to confirm the authenticity of data received and the trustworthiness of the sensor node involved. Thus, trust establishment between nodes is a very important security attribute. The rationale is that false data can alter the predictability of the entire network and the integrity of the data compromised. Thus, data should be protected against alterations and correct/accurate data must be received by end users at all the time [5]. Another important reason why severe security threats exist in WSN is due to the fact that sensor networks interact closely with their physical environment and with people. To this end, the current security mechanisms are insufficient to cope with the limitations and complexities faced by WSNs [19]. These therefore, constitute new research challenges on varieties of issues such as being robust to DoS, privacy, secrecy and authentication, key establishment, routing security and node capture [19]. In general, a critical security challenge is bent on protecting wireless communication links against the onslaught of eavesdropping and tampering. There are also several existing security related problems not discussed in this paper that need further research.

A. *Major WSN Security Challenges*

WSNs have numerous attributes that makes them exceptionally incapable of thwarting several security attacks in the threatening environments like the battlefield in the perspective of the military [20]. They include:

- In WSN a wireless channel/node is open to everyone. Anyone can participate in communication because the configuration of the radio interface is done at frequency band which is constant. This however offer attackers the greatest opportunity to break into WSN.
- Several protocols in WSN are open and consequently, attackers can launch dispatch attacks effortlessly by exploiting the vulnerabilities in the open protocols.
- Due to the existence of constraint resources, it becomes cumbersome to execute effective security algorithms on the sensors environment because some of these algorithms are complex.
- Because WSNs are usually deployed in areas considered to be hostile and without any fixed infrastructure, there are always faced with various attacks. This is due to the difficulty of installing constant surveillance after network deployment.

Moreover, Chen *et al.* [21] summarized several security challenges in WSN which are highlighted as following:

- Reducing the resource consume and increasing the performance of security.
- Sensor networks are more prone to link attacks such as passive eavesdropping, active interfering and so on.
- There is end-to-end information transfer applies intermediate during in-network processing.
- The traditional wired-based security schemes becomes inept by wireless communication characteristics.
- Complexity is introduced by large scale and node mobility.
- Network topology is rendered dynamic due to the addition and failure of nodes.

B. *WSN Possible Attacks*

Security attacks in WSN can be classified into attack techniques, compromised nodes, passive attack, active attack, external attack and internal attack [20]. In a study by Du and Chen [15], four likely attacks were reported that can be targeted on sensor time synchronization. These attacks include replay, message manipulation, masquerade and delay. Furthermore, Saraogi [22] also discussed several security threats and attack types on WSN. Some of the attacks discussed in [22] are the node subversion, collection information, false node, and malicious data. Others are the Sybil, sinkhole attacks and Wormholes. The study also discussed several countermeasure for some of these threats.

1) Attack techniques: Several techniques are employed by attackers to scale attacks on WSN due to lack of knolowled of most of the communication protocols. This is perfomed by eavesdropping on the transmitted packets. In this case, false packets can be secretely inserted into the network to cause sensor nodes confusion. In addition, received packets can also be alter by malicious nodes before being forwarded[20].

2) Node compromisation: This attack constitute one of the most deadliest malicius attacks that targets WSN. This attack takes advantage of the fact sensors networks are deployed in environment considered hostile where constant monitoring are not maintained. Thus, an attacker can seasily pick a sensor node and all imortant information for security protocols can easily be extracted [20].

3) Passive versus active attack: In passive attack, vital security information are extracted in WSN unknowingly. The attacker remains quiet so that it can eavesdrop on the traffic or quietly transformed to a network participant in order to steal vital information in the network such as traffic data in which analysis can be performed upon to to extract some secret information [20]. The information gathered can then be used for different purposes. Passive attack is a very treacherous form of attacks since no traces or evidences are left after the attack. However, the impact of active attacks is much more dangerous than passive attacks. But other anomalies can signify the evidence of malicious attacks in the network since the attacker is a typical and active participant in the network communications [20].

4) External versus internal attack: External attacks originates fom the enviriomENT external to the network. It can be achieved via passive eavesdropping or the insertion of malicious packets into the network with the capability to constantly consuming processing and energy resources. Moreover, internal form of attacks are carried out by nodes assumed to be genuine that will behave in unintended ways [23].

5) Group communication attacks: Cheikhrouhou [24] conducted an indepth discussion on attacks on WSN that emanates from group communication. In this form of attacks, group communication in WSNs are vulnerable to several attacks as a result of the nature or the inherent features of the networks. Some of the group communication attacks as discussed in [24] are sumarized as follows:

- **Replay attack:** In this attack, old messages can be replay by an attacker for the sole purpose of gaining access either a particular group or to distract their operations. In particular, for a successful interception of a vital information of a valid such as authentication information, the attacker can replay the message in order to gain access.
- **Impersonation attack:** This attack operates by imitating the identity of one of the group members in order to gain access or carry out malicious act within the group. In the perspective of WSN, the attacker can gain connection with other nodes or to launch other attacks on behalf of the node.
- **Injecting false message:** In this attack, false or fake messages can be inserted into the nodes to disturb their operation.
- **Eavesdropping:** In this attack, there is passive participation of the attacker in a group communication by eavesdropping transmitted messages. This requires information in critical applications such as healthcare, military operations to be kept secret.
- **DoS attack:** This attack constitute an attempt to stop a group from operating or to disrupt their services by an attacker. DoS attacks can be scaled by an insider or outsider by sending fake group leave request on behalf of other members.

III. SDNs Security Challenges

In this section, we present the security challenges that affects SDNs.

A. SDN in WSN Architecture

SDWSN is a new network paradigm that originates from the combination of the SDN and the WSN. WSN devices that exist are considered to be half duplex since they can only transmit or receives in one given frequency at a given time. Consequently, the in-band control communication between SDN nodes and SDN controller is needed. The aim of the SDWSN was to make network management of WSN flexible and simple and also to enable the central or abstract view of the whole networks.

Jacobsson and Orfanidis [25] proposed a flexible architecture for WSN and IoT that are based on SDN and where in-network processing is an integral part. The reported that the existing SDN architecture for WSN is faced with several challenges. WSN have constrained resources and in most cases they use battery as source of power and this means that the available energy must be well managed. However, one of the basic functions in SDN architecture is the communication between the control and data plane and an increase in the communication will increase the energy consumption. Therefore, energy efficiency is an important factor to be considered in the perspective of SDWSN [25]. SDN is an important building block for being able to use standardized low-cost off-the-shelf hardware and yet achieve customization suitable to the individual deployments.

Luo *et al.* [26] proposed the network paradigm called SDWSN, with architecture showing perfect separation between the control, the forwarding planes and the Sensor OpenFlow (SOF). SOF constitute the core element of SDWSN which is considered a communication protocol standard between the data and control planes. In the SOF architecture, the data plane are the network sensors having the functionalities of flow-based packet forwarding. Furthermore, the control plane houses one or more controllers which is the brain of the network. It control and manages the intelligence of the entire network, perform efficient routing and QoS control [26]. The rationale behind the architecture design was to introduce programmability into the networks by deploying a flow table that are customized based on the user needs on each sensor through SOF as a solution to WSN challenges.

B. Wireless SDN Security Opportunities

In both wireless and wired networks, SDN has the greatest ability to provide an abstract view of network status to an element with the responsibility of detecting the existence of threats and abnormal behaviors [27]. In the wireless networks to detect the presence of attacks such as rogue access point will require the cooperation of the access points in working together to which is expedited by SDN surveillance and control power [27].

C. Main Security challenges in SDN

At the controller-application level, the SDN does not have reliable authentication and authorization mechanisms to enable several parties to have access to the network resources while providing the appropriate protection of these resources [9]. One of the most potential security attacks in SDN is DoS attack. Furthermore, with SDN where there is open interfaces and known protocols to simplify network programming, it becomes easier for attackers to get into the network. With the full knowledge of how to control the network as well as access the controller, the operation of the network can be fast and easily be subverted to the benefit of the attacker [9] OpenFlow architecture of SDN are known to suffer from trust issues on OpenFlow applications because it allows third party development [28]. Moreover, there is a new attack that fingerprints SDN network and launches more efficient resource consumption attacks like DDoS. In general, SDN security vulnerabilities comes from the absence of integration with existing security technologies and the inability to poke around every packet [29]. Chen *et al.* [30] outlined other security challenges on SDN such as forged traffic flows, attack switch vulnerabilities, attack control plane communications, attack controller vulnerabilities and the lack of trust management between applications and controller.

IV. SDWSN Security Challenges

Security constitute an essential tool for every network and SDWSN is not an exception. However security in SDWSN is still at the infant stage and has not received considerable attention. In the literature, several researches have been done and solutions published in the perspective security of SDN and WSN respectively. Some of these security solutions can be applied to SDWSN and some cannot be applied [14]. On the other hand, SDWSN lacks major security components like middle boxes and transport layer security (TLS) which makes it more vulnerable to security attacks [31]. The controller which poses as a single point of failure is the most attacked component in the SDWSN even if though attacks are prominent in the whole network. moreover, DoS attacks and intrusion attacks are among the most popular attacks in SDN-based wireless networks [31]. However, some techniques have been proposed that attempt to mitigate the attacks in SDWSN but have not completely mitigated them[31].

The important advantage of the SDWSN is that it enhances network security with its capability of redirecting or filtering traffic flows based on packet contents or network states [32]. But in the traditional network, such functions normally require additional security modules. In SDWSN they can be naturally supported. In addition, the clear separation between the control and data plane in the SDWSN offers several advantages and on the other hand, introduce more risks which makes the paradigm to become more vulnerable to more attack vectors than the traditional network. Consequently, the security requirement, shown in TABLE I, can be affected hardly by the separation of planes in SDN [32].

TABLE I. Security Requirements of SDN [32]

Requirement	Description
Confidentiality	To prevent information disclosure to unauthorized third parties.
Integrity	To ensure that information is not modified by any adversary. Availability To ensure that authorized users can access data, devices, and services whenever they have the need.
Authenticity	Entities are ensured to actually be the ones they claim to be.
Authorization	Only legitimate users can access resources.
Nonrepudiation	Users cannot deny any action that they have performed.
Consistency	To ensure that flow rules defined by different applications have no conflict.
Fast responsiveness	Security events should be processed in a timely fashion.
Adaptation	To take into account user mobility and dynamic network conditions.

As we stated earlier, some of the threats faced in SDWSN can be adopted from SDN and WSN respectively. TABLE II as analyzed by He *et al.* [32] presents list and discussion of these security threats which are inherent in SDN.

- **Forged or faked traffic flows:** The forwarding devices and the controller are most likely to be endangered by this kind of attack. For instance, an attacker can launch a DoS attack to overwhelm the forwarding devices and the controller resources. Thus, this attack can be mitigated by the authentication mechanisms.

- **Attacks on forwarding devices:** This type of attacks can easily overwhelm the network. In this case, a single forwarding device could be used to discard, slow down, or deviate network traffic. In the worst case, forged requests could be injected to overload the controller.

- **Attacks on control plane communications:** Attacks of this nature can be used to generate DoS attacks or divert flows of network traffic for the purpose of data theft. Several weaknesses have been reported concerning the TLS/SSL communication and the public key infrastructure. Consequently, the controller can be compromised and the security of those communications suffer from a single point of failure, which may be a self-signed certificate or a compromised certificate authority. The TLS/SSL mode alone is insufficient to guarantee the controller and the forwarding devices trust establishment.

- **Attacks on the controller:** This is a serious attack on the SDWSN because a malicious or faulty controller could compromise the entire network.

- **Lack of trust mechanisms between the controller and management applications:** The lack of trust mechanisms result in lack of trusted relationships between applications and controller. This can result in the controller being attacked or failed.

- **Attacks on administrative stations:** This constitute a machine that is used in SDN to access the controller and the threat surface as seen from a compromised machine is even larger.

TABLE II. THREATS INHERITED IN THE SDN [32]

Threat	Consequences in SDWSN
Forged or faked traffic flows	Can be an entryway for DoS attacks.
Attacks on forwarding devices	The effect is possibly expanded.
Attacks on control plane communications	Correspondence with coherently incorporated controllers can be investigated.
Controller attacks	Controlling the controller may trade off the whole system.
Lack of trust mechanisms between the controller and management applications	Compromised applications can now effectively be created and sent on controllers
Attacks on administrative stations	Presently the effect is possibly increased.
Lack of trusted infrastructure for forensics and remediation	It is as yet basic to guarantee quick recovery and finding when flaws happen.

In TABLE II, we present a summary of the threats in SDN which are also applicable to SDWSN. Since security has become critical in the SDN, the security model/framework of the SDWSN must be designed to protect the network itself, the controller plane, the sensors and the protocols used for communication within the network. The network must at all times be alert and aware of any potential threat. In the viewpoint of SDN, Ali *et al.* [33] explained that, SDN security can be enhanced by utilizing the characteristics of its architecture, however, the architecture itself poses a security bottle-neck. In point of view of the of the WSN, Giruka *et al.* [34] highlighted on the issues of sensor networks authentication. Rawat and Reddy [31] stated that each sensor node begins “life” trusting only itself. Consequently, it is therefore important that a node is able to extend such trust to its neighbouring counterparts for the goal of creating a secure network which is achievable using various protocols of authentication. This requires that nodes should be equipped with the capability of protecting themselves in particular and the entire network at large from any node that is considered malicious/compromised via the application of data encryption techniques [34].

Moreover, Akhunzada *et al.* [35] from SDN perspective outlined some of the security vulnerabilities, attacks and security challenges that are inherently common to the control plane. They include packet-in controller manipulation attacks, configuration conflicts, manipulating the system variables, controller capability of proper auditing and authenticating diverse applications.

Padmavathi and Shanmugapriya [36] also classify security threats of the WSNs such as corruption of message, physical attacks, node outage, fake/false node, replication of nodes, collection of passive information and privacy attacks.Though, the SDWSN is a new network paradigm, most existing security requirements are still applicable as summarized in TABLE I.

TABLE III introduces existing work in SDN security, the security solutions using different techniques. Moreover, it present the summary of different algorithms that have been developed by researchers to solve different security aspects of SDN as well as the entire work done, given SDWSN..

TABLE III. SDN SECURITY CHALLENGES AND COUNTERMEASURES

Algorithm name	Security aspect	Techniques Used	Summary
“Novel mechanism for resilience to failures in SDN” [37]	Scaling a man-in-middle attack among switch and the SDN controller	Controller replication	This is a new mechanism implemented as resilience to network failures in the SDN. [37] developed the component to enhace resilience in NOX that uses its component organization. Moreover, a Primary-Backup method was introduced to enhanve the resilience of the SDN.
“SDN-based DDoS blocking scheme” [38]	DoS/DDoS attack specifically on the controller	DDoS Blocking Application	The DDoS blocking scheme is used to protect message exchange among the DDoS blocking application that executes on the controller as well as the server in SDN-managed network. However, everyother interactions are carried out in the interfaces of the standard OpenFlow.
“Virtual source Address Validation Edge (VAVE)” [39]	Launching a DoS attack aim at overwhelming the the Flow Table and Flow Buffer	Integration of Validation mechanism with OpenFlow/NOX architecture.	[39] highlights the important limitations of the SAVI such that bound addresses one of SAVI is still forgable making it difficult for SAVI to be trusted and deployed. However, the problem can be mitigated via a solution called VAVE. According to [39], it constitute the first proposal to be made about a machanism of source address validation with the architecture of the OpenFlow/NOX.
“Flover “[40]	Security rules and configuration conflicts	Flow Verification	[40] proposed proposed a novel approach of modelling OpenFlow flow tables using Yices SMT solver which whether non-bypass property are violated. In addition, a prototype known ad the flow verification tool (FLOVER) was developed. It transforms a given flow table into a series of Yices assertions as well as checking for any inconsistency based on the prevailing security policy of the network.
“NICE” [41]	Illegal access	automating the testing of Open-Flow applications	[41] implemented a tool called NICE which automate the testing of OpenFlow applications using a combination of both model checking and concolic execution. The tool is to expidite the exploration of the state space of the original programs of the controller meant for NOX platform.
“DISCO” [42]	A distributed multi-controllers-based threats	DISCO for WAN control plane and overlay networks	[42] also developed what was called DISCO (DIstributed SDN COntrol plane) for Wireless Area Network (WAN) and overlay networks considered to be guarded. DISCO is organized in a per domain manner, where an individual controller is responsible for specific SDN domain.

V. CONCLUSION

This paper presents several security challenges of SDWSN that originates from the perspective of WSN and SDN. The paper also discuss several existing countermeasures and existing proposed solutions that can be used to mitigate those security challenges. The paper surveyed and performed security analysis of the inheritable security challenges faced by the network paradigm of SDWSN. Based on the survey, we found that SDWSN is still at its infancy stage and security remains the major issue. Therefore, mechanisms to mitigate security attacks in SDWSN must be designed and implemented. Security model/framework must be designed to protect the entire network, the controller plane, the sensors and the protocols used for communication within the network. This is important to ensure that SDWSN is secured and dependable, gain widespread applicability and so on.

Acknowledgment

This work was supported by FRC in the NWU-Mafikeng and the CSIR. We express our sincere appreciation and thanks to them as well as our colleagues in the Computer Science Department.

References

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

[2] A.M. Abu-Mahfouz, G. Hancke, S. Isaac, "Positioning system in wireless sensor networks using NS-2," *Softw. Eng.*, vol. 2, no. 4, pp. 91–100, 2012.

[3] A. De Gante, M. Aslan, and A. Matrawy, "Smart wireless sensor network management based on software-defined networking," *(QBSC), 2014 27th Bienn. …*, 2014.

[4] 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.

[5] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and Challenges in Wireless Sensor Networks," in *International Conference on Machine Intelligence and Research Advancement*, 2013, no. July, pp. 58–62.

[6] A. M. Abu-Mahfouz, T. Olwal, A. Kurien, J. L. Munda, and K. Djouani, "Toward developing a distributed autonomous energy management system (DAEMS)," in *IEEE AFRICON 2015*, 2015, pp. 1–6.

[7] 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.

[8] 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.

[9] S. Sezer, S. Scott-Hayward, and P. Chouhan, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE*, 2013.

[10] T. Grandison and M. Sloman, "A survey of trust in internet applications," *Commun. Surv. Tutorials*, 2000.

[11] 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.

[12] K. Bakshi, "Considerations for software defined networking (SDN): Approaches and use cases," *IEEE Aerospace Conference*, 2013, pp. 1–9.

[13] 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.

[14] 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.

[15] X. Du and H. Chen, "Security in wireless sensor networks," *IEEE Wirel. Commun.*, 2008.

[16] 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.

[17] 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 *Proc of the 14th IEEE International Conference on Industrial Informatics*, 2016, pp. 1166–1170.

[18] 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.

[19] J. Stankovic, "Research challenges for wireless sensor networks," *ACM SIGBED Rev.*, 2004.

[20] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Commun. Surv. Tutorials*, vol. 10.3, no. APA, 2008.

[21] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network security: a survey," *IEEE Commun. Surv. Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[22] M. Saraogi, "Security in Wireless Sensor Networks," *ACM Sensys*, pp. 513–552, 2004.

[23] D. De, O. Gonçalves, and D. G. Costa, "A Survey of Image Security in Wireless Sensor Networks," *J. Imaging*, vol. 1, pp. 4–30, 2015.

[24] O. Cheikhrouhou, "Secure Group Communication in Wireless Sensor Networks: A survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 115–132, 2016.

[25] M. Jacobsson and C. Orfanidis, "Using Software-defined Networking Principles for Wireless Sensor Networks," in *11th Swedish National Computer Networking Workshop*, 2015, no. Sncnw.

[26] T. Luo, H. Tan, and T. Q. S. Quek, "Sensor OpenFlow : Enabling Software-Defined Wireless Sensor Networks," pp. 2–5, 2012.

[27] C. Chaudet and Y. Haddad, "Wireless software defined networks: Challenges and opportunities," , *Commun. Antennas …*, 2013.

[28] H. Farhady, H. Lee, and A. Nakao, "Software-defined networking: A survey," *Comput. Networks*, 2015.

[29] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," *Comput. Networks*, 2014.

[30] J. Chen, X. Zheng, and C. Rong, "Survey on software-defined networking," *Int. Conf. Cloud Comput.*, 2015.

[31] D. Rawat and S. Reddy, "Recent advances on Software Defined Wireless Networking," in *IEEE SoutheastCon*, 2016, pp. 1–8.

[32] D. He, S. Chan, and M. Guizani, "Securing software defined wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 20–25, 2016.

[33] S. Ali, V. Sivaraman, and A. Radford, "A survey of securing networks using software defined networking," *IEEE Trans. Reliab.* , vol. 64, no. 3, pp. 1086–1097, 2015.

[34] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," *Wirel. Commun. Mob. Comput.*, vol. 8, no. 1, pp. 1–24, Jan. 2008.

[35] A. Akhunzada, A. Gani, N. Anuar, and A. Abdelaziz, "Secure and dependable software defined networks" *J. Netw.*, vol. 61, pp. 199–221, 2016.

[36] D. G. Padmavathi and M. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *arXiv Prepr.*, Sep. 2009.

[37] P. Fonseca, R. Bennesby, E. Mota, and A. Passito, "A replication component for resilient OpenFlow-based networking," T*he IEEE Network Operations and Management Symposium*, 2012, pp. 933–939.

[38] S. Lim, J. Ha, H. Kim, and Y. Kim, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," *Ubiquitous Futur.*, 2014.

[39] G. Yao, J. Bi, and P. Xiao, "Source address validation solution with OpenFlow/NOX architecture," *Int. Conf. Netw. Protoc.*, pp. 7–12, 2011.

[40] S. Son, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Model checking invariant security properties in OpenFlow," *IEEE Int. Conf. Commun.*, pp. 1974–1979, 2013.

[41] M. Canini, D. Venzano, P. Peresini, D. Kostic, and J. Rexford, "A NICE Way to Test OpenFlow Applications.," *NSDI*, 2012.

[42] K. Phemius, M. Bouet, and J. Leguay, "DISCO: Distributed multi-domain SDN controllers," in *IEEE/IFIP Network Operations and Management Symp: Management in a Software Defined World*, 2014.