Software Defined Wireless Sensor Networks Management and Security Challenges: *A Review*

Ratanang Thupae
Department of Computer Science
North-West University
Mafikeng, South Africa
ratanangthupae@gmail.com

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

Naison Gasela
Department of Computer Science
North-West University
Mafikeng, South Africa
naison.gasela@nwu.ac.za

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

***Abstract*— Software defined networking (SDN) is a paradigm developed to cope with inherent limitations posed by the lack of flexibility in the traditional networking architecture like the Wireless Sensor Network (WSN). The application of SDN in WSN has been advantageous with respect to network management and configuration leading to a new network paradigm called SDWSN. Despite the benefits, SDWSN is faced with several challenges dominated by network management, security, and scalability. These have prompted several research activities among industrial and academic researchers worldwide. Though several solutions have been proposed or developed, most of the challenges still exist and more research works are needed to address them. Therefore, this paper presents a review of the challenges of SDWSN in the aspects of network management, security and its application on Internet of Things (IoT). The essence is to comprehend the existing challenges in an effort to find effective and efficient solutions to ensure more secure, dependable and energy efficient SDWSN. We reviewed several literature on WSN, SDN and SDWSN and presented the findings in the form of challenges and solutions. The analysis shows that SDWSN challenges originates from SDN, WSN and the technology is still at its early stage, though is developing.**

Keywords— WSN, SDWSN, Network management, Security.

I. INTRODUCTION

Software defined network (SDN) is a network paradigm which is promising in terms of network management and its configuration due to the decoupling of the control and the data plane as well as programmability. In SDN, network management policies are translated into packet forwarding rules by the centralized controller and deploy to devices of the network such as the switches, sensors, and routers [1]. SDN has been advantageous since its inception and has been applied in several areas and applications such as in wireless sensor networks (WSNs) due to its cost-effective approach in network management and control. In the realm of WSN, SDN goal is to address the challenges and inflexibility that affects the traditional network architecture. WSN is faced with several challenges which is based on application and functions such as environmental observation or security attacks due to recent explosion in terms of usage [3]. Moreover, with the sensor nodes, it is hard after deployment to change their behaviour which constitute a challenge. WSN‘s operation is affected by so many familiar inter-related factors such as network topology, network traffic flows and communication protocols [4]. Thus, SDN in WSN is geared towards addressing these challenges resulting to a new network paradigm known as software defined wireless sensor network (SDWSN). Hassan *et al*. [5] stated that SDWSN is introduced in WSN to play a critical role for sensor nodes through communication and the deployment of the network. It offers flexible behaviour and its potential is significant to serve the infrastructure of WSN. Other challenges that need researcher’s attention in WSN and SDN is security and quality of service (QoS) [6]. QoS requirements plays a huge role due to its diversity on several applications. Since SDN paradigm is so trending based on the recent technologies, the objective is to speed up network management [7][43]. However, new challenges are brought to the network management and resource scheduling due to poor routing designs and so on. Moreover, network with limited resources and unclear routing schemes may cause congestion of traffic which could lead to the degradation of network performance and QoS.

The birth of SDWSN is beneficial for several application such as in environmental observation or systems of security and also in the scaling up of WSNs [3] [8]. In spite of these benefits, SDWSN is marred with several challenges that originates from both SDN and WSN [9]. Some of these challenges include security, energy inefficiency, traffic engineering and network management like virtualization, orchestration, programmability, dynamic scaling, visibility, automation and so on. Several solutions have also been presented in different forms to address the challenges. However, some of the challenges still persist. One critical aspect that requires urgent attention is on improving SDWSNs’ energy consumption especially in routing protocols and network management as well as overcoming Internet of Things (IoT) problems. Therefore, this paper brings together some of the potential challenges in SDWSN and countermeasures already proposed. To achieve this, we reviewed and analysed some of the related works and also presented summary of the identified challenges.

The remaining parts of the paper is organized as follows: Section II presents the analysis of the existing works, Section III presents the issues in SDWSN, Section IV is the paper discussion and Section V is the conclusion.

II. Related Works

This section presents some of the related works that have performed on the issues of SDWSN specifically on network management and security. De Gante *et al.* [10] reported that network management involved a complex process, as such, the need for proper configuration, provisioning and management. Moreover, to ensure efficient network, there are many principles that need to be followed and implemented. That is, for a good network management to be achieved, the design of efficient architectures is still an unresolved challenge to the research community.

Modieginyane *et al*. [7] presented issues concerning efficiency of network management in the WSN perspective. They found that since SDWSN is still an emerging paradigm, efficient network management needs more attention. They suggested an implementation strategy that is based on the programmability of the network and propose method of implementing simple state on the sink node. Moreover, the study stated that several issues affecting the SDN-OpenFlow southbound and northbound interfaces. Kgogo *et al*. [11] reviewed on some of the security faced by SDWSN as well as several security issues of inherent from SDN and WSN. Based on the findings, they suggested that efficient security framework has to be designed for protection of the whole SDWSN. Furthermore, in order to ensure a secure communication in a network, the requirements of confidentiality, integrity, and availability on information, non-repudiation and authentication should be considered.

Pritchard *et al*. [12] presented several security issues that affects the SDWSN and its impact in the management of WSN. However, in SDWSN the controller handles the control logic of WSN while the data transmission functionality is handled by the device. Since sensor nodes carry out data forwarding operations, the task of network resource computation is handled by the controller without more resources like energy being consumed. Some of the benefits of SDN in WSN include promoting interoperability, improving sustainability and efficiency. They went further to suggest that for a secure network and proper management in SDWSN, merging of SDN and WSN solutions could lead to realization of critical impact in the development of IoT paradigm especially in the configuration of accurate traffic flow. Consequently, Kobo *et al.* [9] performed a survey and presented challenges of the SDWSN. Their study found that due to device constraints, several challenges such as energy, limited computational capability and so on, makes it difficult for sensor nodes to be networked. The suggested that, based on the design requirements of SDWSN, evaluation and attention is needed since SDWSN model is still developing. Sood *et al*. [13] highlighted on traditional network tools, storing, processing and forwarding large efficient data is the critical need for future IoT using SDWSN since it can simplify the network control and management. They identified several challenges and opportunities that can arise for IoT coming from SDWSN perspective in order to accurately classify traffic on the entire network.

III. SDWSN Challenges and Solutions

This section presents some of the challenges in the SDWSN in terms of network management and security. They are discussed as follows.

A. Network Management Systems

In SDN and SDWSN, network management is a complex challenge and is studied in terms of load-balancing, fault tolerance, traffic analysis and so on. They constitute the procedures and other important aspects to control the operation of the network [14]. The challenge of inefficient network management posed to SDN is serious and needs to be addressed in order to significantly improve the utilization of resources for best performance achievement. Accordingly, the architecture should be designed with the capability of classifying different traffic types for different applications. Furthermore, to ensure network traffic accuracy and timely statistics at different abstraction levels, management applications are needed [15, 16]. The important tool in network management is network monitoring. It has also been reported that the problems of network management emanates from the WSN. Since in the traditional networks, the primary goal is to minimize response time, sensor networks goal is to reduce energy usage [17]. The management of WSN is a new interesting research area that has recently gained considerable attention from the research community. However, set of important management challenges have already been addressed.

Furthermore, Yu *et al.* in [4] stated that for the solutions to the identified challenges, several management features will appear in the future management architecture since it aim to maintain the availability and improve network performance. Some of the challenges outlined in the perspective of network management are discussed. The problems encountered in network management in the perspective of SDN and WSN include the development of general purpose network management layer protocols which is still largely an unexplored area for WSNs, the design for efficient network management architecture, network state that continuously change, network configuration based on low-level per device, network appliances which are specialized or middle-boxes which poses reliability threats, topology modifications that requires human intervention and dynamic traffic isolation (DTI). [4, 14].

Huang *et al.* [18] proposed SDWSN prototype for the improvement of energy efficiency and adaptability of the monitoring systems in WSN. Based on this proposal, a network monitoring system that operates with machine learning (ML) techniques in artificial intelligence (AI) was developed. In addition, Wang *et al*. [19] proposed sleep scheduling algorithm called SDN-ECCKN in SDN. It was designed with the control of reducing the total time it takes the network transmit information and the maintenance of such connectivity. Based on the algorithmic computation, the controller was given the task of network functioning due to the absence of sensor to sensor propagation in the algorithm. Moreover, Akyildiz *et al.* [15] proposed two solutions based on the network management which are the query-based monitoring that operates based on the request or response technique. The approach periodically

activates the switch on each active flow to collect flow-level statistics. It produced high accuracy but generate high overheads. On the other hand, the push-based monitoring is based on the published or subscribed or distributed techniques. In this approach, the server automatically deliver information to clients. However, the number of client requests handled by the server can be reduced. Also, a monitoring tool was implemented using a server considered to be dedicated which is separated from the controller of the network. The solution is capable of ensuring accurate traffic monitoring having low latency, while still significantly plummeting overheads of processing incurred by the controller during flow statistics collection. Thus, network management in SDN is a challenge due to scalability issues originating from controller capacity, low latency to control path [15]. Gibb *et al.*[20] argued that based on the problem of specialized hardware in the process of network deployment, this middle-boxes should not be placed at network locations where all traffic must visit the check points. They further explained that it raises some concerns such as efficiency, robustness and correctness and their proposed solution was based on SDN and OpenFlow can be utilized to overcome the issue of (DTI).

TABLE I. COMMON THREATS AND ATTACKS

Ref.	Security Threats & Attacks	Objective
[40-42]	Threat to physical attack.	Utilization of side channel analysis for physical destruction of sensor nodes.
	Node or base station capture.	To capture and compromise a sensor node.
	Privacy experiencing a threat.	To access different types of personal information utilizing WSN's vulnerability.
	Threats of attack in terms of application.	DoS directed against any normal service and operating systems.
	Routing mechanism and transmission channel experiencing threat of attack.	Prevents routing and channel between sensor nodes.
	Link level experiencing threat of attack.	Message forgery and information alteration to eavesdrop on a wireless channel.

Based on the issue of network management in SDN and WSN the following are identified as communicating factors such as traffic and fault tolerance, scalability, performance, adaptability, reliability, traffic management and energy efficiency. These challenges can negatively affects the entire network if they are not given attention during the design phase. They are discussed as follows:

1) Fault and traffic tolerance: These issues are experienced due to the proneness of WSN to network dynamics such as packets dropping and so on. Thus, to guard against it, management system should act with resistant to the network dynamics via reconfiguration of the network [21]. In the perspective of WSN, failures ranging from sensor nodes to communication can occur at any time without pre warning which poses a critical challenge to the network. However sensor application design have already been taken into consideration. In the event of failure, WSN still need to be able to reconfigure and recover to normal functioning without human intervention especially in restricted environments [4]. On the other hand, to endure unusual traffic, traffic tolerance should be enabled while still maintaining its expected behaviour. Thus, issues of legitimate or illegitimate network traffic management as well as malicious attacks are dealt by traffic tolerance.

2) Scalability, reliability, adaptability and performance: Akyildiz *et al*. [22] states that the specified approaches in the control and data plane can be helpful with the trade-offs between latency and load balance under scalability and availability. This study considered the important issues of scalability confronting SDN that require insights. These issues include resilience to failures based on network performance, flow-setup overhead and increased load on the controller. Furthermore, the following are considered as the key issues that affects scalability in SDN such as extensibility, behavioural and programming abstractions. Based on them, Ethane [23] was a proposed, where the controller is charged with the installation of switch forwarding state based on flow base. Most of these issue can be addressed without losing SDN benefits [24]. However, there is still an argument that SDN scalability still poses as an issue due to wrongful assumptions about the decoupling nature of the data and control planes. Consequently, a viable solution in the form of a proactive design called DIFANE was proposed in [25]. For the system to operate efficiently and adaptable, it should be equipped with the capabilities of retrieving states of the current network [21]. Accordingly, a comparison of the performance was conducted to assess the best performing SDN controller and protocol for developing SDN [26]. Modieginyane *et.al* and Kim *et al.* [27, 28] stated that DIFANE and DevoFlow were proposed as solutions to resolve the performance and scalability challenges which was possible via various algorithms and mechanisms. Also, Yeganeh *et al*. [24] re-constructed the issues of scalability that confronts SDN. However, they argued that the issues are not only limited to SDN alone. In the perspective of reliability issues in the data plane, a fast failure recovery mechanisms was suggested for implementation. Thus, performance, adaptability and scalability issues need to be fully given the desire attention.

3) Energy efficiency: Energy efficiency can be simply defined as reduction of energy usage by devices e.g. routing protocols. However, since nodes in WSN are always energy constraint devices, they pose restrictions to the design, sensor applications and also implementation of network protocols [10]. Moreover, due to economy and environmental security in WSN, the reduction of energy consumption still remains an important issue for discussion in recent and future years [29]. Several researchers have suggested that SDN can be a promising way for sensor network management in terms of energy efficiency. Thus, by effectively preventing the transmission of unnecessary loads, the energy efficiency can be improved [26].

B. Security

SDN is a networking approach aiming to simplify network configuration and management [12]. SDN ensure flexibility

TABLE II. SUMMARY OF CHALLENGES AND SOLUTIONS IN THE SDWSN

Ref.	Challenge	Approach	Tool	Proposed Solution
[15]	Network Management (Traffic engineering)	SDN TE	Wildcard rules	Query based and Push based monitoring.
[20]	Network Management (Middle-Boxes)	Chokepoints	OpenFlow switches	Waypoint services.
[36]	Network Management- (Middle-Boxes)	Chokepoints	OpenFlow switches	Software centric, separated hardware and software.
[37]	Network Management (Middle-Boxes)	Chokepoints	OpenFlow switches	Architectural design where enterprises depend on service providers based on middle-box to subcontract of the traffic has to process.
[38]	Network Management (Middle-Boxes)	Regular switches which move the controller's complexity	OpenFlow switches	PLayer which consist of several switches that route traffic to middle-boxes.
[18]	Energy efficiency	Machine Learning (ML) technique	-	Cognitive SDWSN prototype to monitor network system using Reinforcement Learning (RL) Algorithm
[19]	Energy efficiency	OpenFlow controller/Control plane	-	Sleep scheduling algorithm to reduce the total running time of network in terms of transmission and also maintain the network connectivity.
[4]	Fault tolerance (Sensor and Communication nodes)	-	-	-
[39]	Scalability (Resilience to failures based on network performance, Flow setup overhead and Increased load on the controller) and Performance.	SDN controller and protocol for development of SDN was the approach for performance.	-	DIFANE and DevoFlow with various algorithms
[32]	Security (DoS and DDoS, Authentication and, Authorization)	OpenFlow controller	-	FRESCO[32] for transport layer security and secure sockets layer

and eliminates the inherent challenges faced by traditional network architectures. However, the benefits also comes with the introduction of new threats and attack channelled towards the different planes of the SDN to compromise its security [12]. Kreutz *et al.* [30] in their study highlights several security attacks and threats as problems that always affects SDN. Accordingly, Ahmad *et al.* in [31] outlined these security threats and they were further categorized by planes which also accommodates SDN applications such as network management and so on. Moreover, since security is significant when a sensor of a network is re-formed, the following are the main points regarding the network security management in WSN; the keeping of monitored database that look at the environment of operation, the status of the security and the information for local nodes, remotely analysing sensed data, topology, node, routing status, and other security parameters received or collected and making a revision of sensor node's configuration information, the routing topology and security parameters using a control channel in the event of abnormal node status detection.

With the emergence of SDSWN, sensors are known to carry out forwarding operations and the network computations are done by the controller without negatively affecting the consumption of energy [7]. As stated by Ahmad *et al.*[31], some of the challenges originating from security includes: in application plane authentication and authorization have been identified as important challenges. In addition, the controller plane houses the network control logic and has been highly targeted my malicious attackers. Some of the attacks are the DoS which can be launched on the vulnerability of the control plane communication to steal data as well as the launching of DDoS attacks using many switches under the attacker's control. Therefore, transport layer security and secure sockets layer lack trust due to communication resulting to leakage of data during traffic of the network.

Till date, several solutions have been developed to address the challenges in the SDN. For instance, FRESCO [32] was proposed to allow the applications of security to be implemented on any controller of the OpenFlow. However, authentication and authorization still remain a serious issues prompting some application layer security solutions to incorporate validation and verification models to ensure that there are no new created policies conflict with some specific properties of the controller [9]. Ahmad *et al.* [31] also proposed several approaches to secure the control plane such as maintaining security against faulty/malicious applications, scalability target of the control plane, the prevention of DoS or distributed DoS, and ensuring of a reliable security via controller. However, inter-operability with combination of other networks which can improve WSN's efficiency and sustainability should to be taken into consideration. In terms of security, the nature of WSN requires plethora of wireless sensor nodes to be equipped with security abilities. Furthermore, since WSN is composed of large number of sensors which are deployed over a sensor network to areas that are difficult to assess, security requirements need to be considered in its design such as authentication, confidentiality, integrity and non-repudiation

C. Internet of Things

Today WSN is a trending enabled technology for IoT because they are introduce new aspects in terms of application of WSN integrated to the traditional infrastructural Internet [33][44]. In terms of information collection and sharing, IoT devices are equipped with the capability of performing analysis, observation and taking intelligent decisions [34]. However, the advent of the IoT in WSN is also faced with several challenges in which one is the inability to effective classify traffic particularly, in enterprise networks. Thus, the classification of scalable and accurate traffic is a problem and is still hard to solve due to non-provisioning of good QoS of all applications that runs on their network [35]. Consequently, SDN can be employed to provide solution to ensure that data is processed in real-time more effectively since the problem lies in the nature of the IoT itself. Moreover, it can also be used to overcoming issues of scalability and reliability.

IV. Discussions

In this paper, we have highlighted some of the existing challenges that are faced by SDWSN and the proposed solutions. We found that SDWSN is faced with several issues in network management, security and so on which were inheritable from the SDN and the WSN. Table I presents some of the security threats and attacks and Table II captures the existing challenges in the aspect of network management, fault tolerance, scalability, security and energy efficiency.

Security is one of the important challenges found in SDN. This challenge exist because security features were not considered in its initial architectural design. In the perspective of fault tolerance, several researchers are still faced with the problem of reliability and resiliency after the architectural design. The reliability of the controller and the devices poses serious threats to the entire network. SDWSN is implemented to facilitate the process of network management; however, designing an efficient network management architecture is considered one of the greatest challenges faced since it continuously support WSNs with services for various sensor applications. Moreover, it is also argued that the SDN introduction can help solve some of the difficulties confronting WSN such as energy efficiency and network management which raise questions like:

1) *Is there still the need to introduce distributed controller?*

2) *What will be the disadvantage in terms of performance and energy consumption of the sensor network if being affected?*

3) *What will be the effect to the controller if malicious attacks are directed towards it?*

4) *If controller is maliciously attacked, what will happen to the entire networks?* [45].

Moreover, De Gante *et al.* [10] emphasized that for further research investigation on WSN in terms performance, reliability, and security especially in IoT, network management or other aspects, more attention should be geared towards assessing their impact on the network. Other issues faced by most systems are fault tolerance, adaptability, scalability, performance, interoperability etc. Yeganeh *et al.*[24] reiterated that scalability remains an issue but is not uniquely fundamental to SDN. However, some of these problems could be addressed without losing the benefits associated with the SDN. Furthermore, to simplify the management of the network with SDN, middles-boxes deployment has been proposed. This is to ensure effective correctness, robustness, efficiency and dynamic updates of the network topology which poses a serious challenge. As a future direction, network management using middles-boxes as waypoint services need to be extended to deal with network performance where issues are raised due to the usage of software to perform encryption. Thus, hardware like the NetFPGA card could be utilized to achieve better performance and speedy. Additionally, the network choke point could be made simple and only use specialized features for a particular traffic.

V. Conclusion

SDWSN is a networking paradigm to ease network management and control in the WSN. Though the technology is beneficial, it also faced with several challenges. This paper presented some of the challenges it inherited from the SDN and WSN. We conducted a review of the challenges and some of the proposed solutions in the literature on the aspects of network management, security and its application in the area of IoT. The basis of the review is to comprehend these challenges and proposed solutions in order develop new efficient approaches to address some of the challenges. We analysed the findings and presented them. Based on our findings, it shows that SDWSN is still at its developmental stage and is faced with several issues such as network management, security, scalability, reliability and energy efficiency. These issues still remains the major issues that need lots of attention from researchers both in the industry and the academia. Thus, more techniques need to be designed, implemented and validated in the SDWSN to make more secure, scalable, reliable, applicable and energy efficient. The future work is to provide solutions to some of the identified challenges in an efficient way.

Acknowledgment

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

References

[1] Huang, H., et al., Joint optimization of rule placement and traffic engineering for QoS provisioning in software defined network. IEEE Transactions on Computers, 2015. **64**(12): p. 3488-3499.

[2] Gau, R.-H. and P.-K. Tsai. SDN-based optimal traffic engineering for cellular networks with service chaining. in Wireless Communications and Networking Conference (WCNC), 2016 IEEE. 2016. IEEE.

[3] 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.

[4] Yu, M., H. Mokhtar, and M. Merabti. A survey of network management architecture in wireless sensor network. in Proceedings of the Sixth Annual Post-Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting. 2006.

[5] Hassan, M.A., Q.-T. Vien, and M. Aiash, *Software defined networking for wireless sensor networks: a survey*. Advances in Wireless Communications and Networks, 2017. **3**(2): p. 10-22.

[6] Qi, W., et al., A traffic-differentiated routing algorithm in Flying Ad Hoc Sensor Networks with SDN cluster controllers. Journal of the Franklin Institute, 2017.

[7] Matlou Omolemo Godwill, A.M.Abu-Mouhfaz, "Utilising Artificial Intelligence in Software Defined Wireless Sensor Network," in *the 43rd IEEE conference of Industrial Electronic Society*, 29 October – 1 November, Beijing, China, 2017, pp. 6131-6136

[8] Kaur, E.Y., et al., *Briefing: Images and Image Processing.* International Journal of Engineering Science, 2017. .

[9] 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.

[10] De Gante, A., M. Aslan, and A. Matrawy. Smart wireless sensor network management based on software-defined networking. in Communications (QBSC), 2014 27th Biennial Symposium on. 2014. IEEE.

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

[12] 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.

[13] Sood, K., S. Yu, and Y. Xiang, Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet of Things Journal, 2016. **3**(4): p. 453-463.

[14] Lara, A., A. Kolasani, and B. Ramamurthy. Simplifying network management using software defined networking and OpenFlow. in Advanced Networks and Telecommuncations Systems (ANTS), 2012 IEEE International Conference on. 2012. IEEE.

[15] Akyildiz, I.F., et al., Research challenges for traffic engineering in software defined networks. IEEE Network, 2016. **30**(3): p. 52-58.

[16] Winnie, L., D. Amitava, and C. Rachel, *Network management in wireless sensor networks.* Management, 2007. **4**(6): p. 1859-1873.

[17] Zhang, J. and V. Varadharajan, *Wireless sensor network key management survey and taxonomy.* Journal of Network and Computer Applications, 2010. **33**(2): p. 63-75.

[18] Huang, R., et al., Energy-efficient monitoring in software defined wireless sensor networks using reinforcement learning: A prototype. International Journal of Distributed Sensor Networks, 2015. **11**(10): p. 360428.

[19] Wang, Y., et al., *An energy-efficient SDN based sleep scheduling algorithm for WSNs.* Journal of Network and Computer Applications, 2016. **59**: p. 39-45.

[20] Gibb, G., H. Zeng, and N. McKeown. Initial thoughts on custom network processing via waypoint services. in WISH-3rd Workshop on Infrastructures for Software/Hardware co-design, CGO. 2011.

[21] Zhang, B. and G. Li. Survey of network management protocols in wireless sensor network. in E-Business and Information System Security, 2009. EBISS'09. International Conference on. 2009. IEEE.

[22] Akyildiz, I.F., et al., *A roadmap for traffic engineering in SDN-OpenFlow networks.* Computer Networks, 2014. **71**: p. 1-30.

[23] Casado, M., et al. Ethane: Taking control of the enterprise. in ACM SIGCOMM Computer Communication Review. 2007. ACM.

[24] Yeganeh, S.H., A. Tootoonchian, and Y. Ganjali, *On scalability of software-defined networking.* IEEE Communications Magazine, 2013. **51**(2): p. 136-141.

[25] Yu, M., et al., *Scalable flow-based networking with DIFANE.* ACM SIGCOMM Computer Communication Review, 2010. **40**(4): p. 351-362.

[26] Modieginyane, K.M., R. Malekian, and B.B. Letswamotse, *Flexible network management and application service adaptability in software defined wireless sensor networks.* Journal of Ambient Intelligence and Humanized Computing, 2018: p. 1-10.

[27] Curtis, A.R., et al. DevoFlow: scaling flow management for high-performance networks. in ACM SIGCOMM Computer Communication Review. 2011. ACM.

[28] Kim, H. and N. Feamster, *Improving network management with software defined networking.* IEEE Communications Magazine, 2013. **51**(2): p. 114-119.

[29] Shu, Z., et al., Traffic engineering in software-defined networking: Measurement and management. IEEE Access, 2016. **4**: p. 3246-3256.

[30] 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.

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

[32] Shin, S., et al. FRESCO: Modular Composable Security Services for Software-Defined Networks. in NDSS. 2013.

[33] Mainetti, L., L. Patrono, and A. Vilei. Evolution of wireless sensor networks towards the internet of things: A survey. in Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on. 2011. IEEE.

[34] Tayyaba, S.K., et al., Software-defined networks (SDNs) and Internet of Things (IoTs): A qualitative prediction for 2020. network, 2016. **7**(11).

[35] Roughan, M., et al. Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification. in Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. 2004. ACM.

[36] Sekar, V., et al. The middlebox manifesto: enabling innovation in middlebox deployment. in Proceedings of the 10th ACM Workshop on Hot Topics in Networks. 2011. ACM.

[37] Sherry, J., et al., *Making middleboxes someone else's problem: network processing as a cloud service.* ACM SIGCOMM Computer Communication Review, 2012. **42**(4): p. 13-24.

[38] Joseph, D.A., A. Tavakoli, and I. Stoica. A policy-aware switching layer for data centers. in ACM SIGCOMM Computer Communication Review. 2008. ACM.

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

[40] Lee, B., S. Bae, and D. Han. Design of network management platform and security framework for WSN. in Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on. 2008. IEEE.

[41] Ngai, E.C., J. Liu, and M.R. Lyu. On the intruder detection for sinkhole attack in wireless sensor networks. in Communications, 2006. ICC'06. IEEE International Conference on. 2006. IEEE.

[42] Qian, Y., K. Lu, and D. Tipper, *A design for secure and survivable wireless sensor networks.* IEEE wireless communications, 2007. **14**(5).

[43] S.W. Pritchard, G.P. Hancke and A.M. Abu-Mahfouz, "Cryptography Methods for Software-Defined Wireless Sensor Networks," in *the 27th International Symposium on Industrial Electronics*, 12-15 June, Cairns, Australia, pp. 1257-1262, 2018.

[44] Godfrey A. Akpakwu, Bruno J. Silva, Gerhard P. Hancke, and Adnan M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 5, no. 12, pp. 1-29, 2017

[45] Hlabishi I. Kobo, Gerhard P. Hancke and A.M. Abu-Mahfouz, "Towards A Distributed Control System For Software Defined Wireless Sensor Networks," in *the 43rd IEEE conference of Industrial Electronic Society*, 29 October – 1 November, Beijing, China, 2017, pp. 6125-6130.