



**UNIVERSITY OF NAIROBI**  
**DEPARTMENT OF COMPUTING AND INFORMATICS**

**USE OF SOFTWARE-DEFINED NETWORKING  
MODEL TO IMPROVE SECURITY IN MIPV6**

**BY:**  
**OKUNDI ELIAKIM OLOGI**

**A research project report submitted to the Department of Computing and Informatics in partial fulfillment of the requirements for the award of the degree of Master of Science in Distributed Computing Technology of the University of Nairobi.**

**AUGUST 2022**

## DECLARATION

I declare that this project is my original work and has not been presented for a postgraduate degree at another University.


Sign: 

Date: 04-AUG-2022

Okundi Eliakim Ologi

P53/38779/2020

This project report has been submitted for examination towards fulfillment for the award of Master of Science in Distributed Computing Technology with my approval as the university supervisor.

Sign: 

Date: 07-Aug-2022

Dr. Stephen Mburu

Department of Computing and Informatics

Faculty of Science and Technology

University of Nairobi

## **ACKNOWLEDGMENT**

I am deeply indebted to my mentors Dr. Stephen Mburu and Mr. Christopher Moturi for their guidance, patience, and insightful input from the commencement of this project to its completion.

I wish to express my appreciation to the Department of Computing and Informatics, and all my lecturers without whose enormous contributions to coursework, this work would have not been possible.

I am grateful to my beloved wife, Grace. Her cooperation, encouragement, patience, understanding, and prayer spurred me on to the successful completion of the project.

My former workmates Brian Ochieng and Phelix Olonde gave me great support and motivation during the building of the simulated network designs.

Finally, and most importantly, I wish to express my deep and heartfelt appreciation to the Almighty God who has graciously made it possible for me to make this important milestone in life.

## ABSTRACT

As networks grow in size, they become complex in design, and security. Management also becomes more pronounced. Over the years, such networks have evolved from traditional networks to those that can be smartly controlled through programmability. Traditional networks experience many security threats such as Sniffing and Distributed Denial of Service (DDoS). Specifically, these attacks are common in mobile networks such as Mobile IP version 6 (MIPv6). The study, therefore, sought to find out how Software-Defined Networking (SDN) model could be used to contain the security threats in the MIPv6 environment. In this research three interrelated perspectives were supported in the use of the software-defined networking model to contain the two security threats in MIPv6: the software-defined networking model perspective (which dealt with how wireless networking components are programmed and coordinated to achieve synchronicity in managing network resources); device mobility perspective (which looked at how the wireless network components such as laptops, tablets, iPads, and mobile phones move from one access point to the next as they acquire and re-acquire IP addresses); and traditional network model perspective (which dealt with the fact that the wireless network devices are managed independently without any programmability or central coordinating components). The three perspectives enabled testing of the hypotheses. Lab experimental design was adopted for the research. The results showed that sniffing and DDoS attacks could be contained through the use of a Software-Defined Networking model. It was observed that in traditional models where there were no Software-Defined Networking controllers, such networks were prone to sniffing and DDoS attacks. The finding agreed with the hypothesis that traditional network models could be compromised by both the DDoS and sniffing attacks as in the case of MIPv6. In the event of an attack, the SDN controller could disable the compromised components of the network. Hence saving the network from more negative effects. Further, the use of both the control plane and the data plane to segregate network data routing functions from routing decisions also made the SDN a better model for containing security challenges in MIPv6. The study found out that many of the security issues related to SDN networks were similar to those experienced in traditional networks. The study noted that the use of the SDN model had far-reaching benefits in improving network security as compared to the legacy or traditional models. The SDN approach enabled coordinated monitoring and management of forwarding policies among distributed network components, resulting in a more flexible management process. The study validated that separation of the control and data planes in the software-defined networking model enabled multi-tenancy and programmability in networks and introduced centralized management into the MIPv6 network architecture. The finding of the study would be helpful in the formulation of policies around network security measures not only in wireless topologies, but also in wired and hybrid topologies.

# TABLE OF CONTENTS

<b>DECLARATION</b>	ii
<b>ACKNOWLEDGMENT</b>	iii
<b>ABSTRACT</b>	iv
<b>LIST OF FIGURES</b>	vii
<b>LIST OF TABLES</b>	viii
<b>ACRONYMS</b>	ix
<b>DEFINITION OF TERMS</b>	x
<b>CHAPTER ONE: INTRODUCTION</b>	1
<b>1.1 Background</b> .....	1
<b>1.2 The Concept of Software-defined Networking</b> .....	2
<b>1.2 Research Problem</b> .....	3
<b>1.3 Research Objectives</b> .....	4
<b>1.4 Value of the Study</b> .....	4
<b>1.5 Motivation for the Research</b> .....	5
<b>CHAPTER TWO: LITERATURE REVIEW</b>	6
<b>2.1 Introduction</b> .....	6
<b>2.2 Theoretical Framework of the Study</b> .....	6
<b>2.3 Conceptual Framework of the Study</b> .....	8
<b>2.4 Empirical Framework</b> .....	14
<b>CHAPTER THREE: RESEARCH METHODOLOGY</b>	15
<b>3.1 Introduction</b> .....	15
<b>3.2 Research Model and Hypothesis Formulation</b> .....	15

<b>3.3 Research Design</b> .....	16
<b>3.4. The Population and Sampling Methods</b> .....	17
<b>3.5 Methodology</b> .....	19
<b>3.6 Data Collection</b> .....	26
<b>3.7 Data Analysis</b> .....	28
<b>3.8 Reliability and Validity</b> .....	28
<b>3.9 Ethical Considerations</b> .....	29
<b>3.10 Summary of Methodology</b> .....	30
<b>CHAPTER FOUR: DATA ANALYSIS, FINDINGS, AND DISCUSSION</b>	<b>31</b>
<b>4.1 Introduction</b> .....	31
<b>4.2 Data Analysis</b> .....	31
<b>4.3 Research Findings</b> .....	34
<b>4.5 Discussion of Findings</b> .....	40
<b>CHAPTER FIVE: SUMMARY, CONCLUSION, AND RECOMMENDATIONS</b>	<b>42</b>
<b>5.1 Introduction</b> .....	42
<b>5.2 Summary of Findings</b> .....	42
<b>5.3 Conclusion</b> .....	44
<b>5.4 Recommendation for Policy and Practice</b> .....	45
<b>5.5 Limitations of the Study</b> .....	46
<b>5.6 Suggestions for Further Study</b> .....	47
<b>REFERENCES</b>	<b>48</b>

## LIST OF FIGURES

Figure 2.1: Conceptual model of an SDN-controlled network.....	10
Figure 2.2: The SDN layered architecture.....	10
Figure 2.3: The MIPv6 Architecture.....	13
Figure 2.4: A road map of different studies on security, privacy, and trust in M-IoT.....	16
Figure 3.1: Flow Diagram of Proposed Process.....	22
Figure 3.2: Network Topology without SDN.....	23
Figure 3.3: Network Topology with SDN.....	25
Figure 4.1: Sniffing Attack without SDN.....	33
Figure 4.2: Sniffing Attack with SDN.....	33
Figure 4.3: DDoS attack without SDN.....	34
Figure 4.4: DDoS attack with SDN.....	34
Figure 4.5: Graph of packet flow for sniffing attack with and without SND.....	38
Figure 4.6: Graph pf packet flow DDoS attack with and without SDN.....	39

## LIST OF TABLES

Table 3.1: Summary of Network Components.....	21
Table 3.2: Packet flow per unit time for sniffing attack without SDN.....	28
Table 3.3: Packet flow per unit time for sniffing attack with SDN.....	28
Table 3.4: Packet flow per unit time for DDoS attack without SDN.....	28
Table 3.5: Packet flow per unit time for DDoS attack with SDN.....	28



## ACRONYMS

<b>AP</b>	- Access Point
<b>BGP</b>	- Border Gateway Protocol
<b>BSSID</b>	- Basic Service Set Identifier
<b>BU</b>	- Binding Update
<b>CN</b>	- Correspondence Node
<b>CoA</b>	- Care of Address
<b>HA</b>	- Home Address
<b>IDS</b>	- Intrusion Detection System
<b>IETF</b>	- Internet Engineering Task Force
<b>IPSec</b>	- Internet Protocol Security
<b>LVAP</b>	- Light Virtual Access Point
<b>IPv4</b>	- Internet Protocol version 4
<b>MIPv6</b>	- Mobile Internet Protocol Version 6
<b>NF</b>	- Network Function
<b>ONP</b>	- Open Network Foundation
<b>OSPF</b>	- Open Shortest Path First
<b>RARP</b>	- Reverse Address Resolution Protocol
<b>SDN</b>	- Software Defined Networking
<b>SDWN</b>	- Software-Defined Wireless Network
<b>SOC</b>	- Service Operation Center
<b>TCP/IP</b>	- Transport Control Protocol/Internet Protocol
<b>WLAN</b>	- Wireless Local Area Network

## DEFINITION OF TERMS

TERM	DEFINITION
<b>Distributed Denial of Service Attack:</b>	A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a high volume of Internet traffic.
<b>Light Virtual Access Point:</b>	A dynamically assigned to a physical access point near the current location of the terminal.
<b>Local Area Network:</b>	A computer network that links devices within a building or a group of adjacent buildings with a radius of less than 1 km.
<b>Mobile IP v6:</b>	The protocol developed as a subset of Internet Protocol version 6 to support mobile connections.
<b>Software-Defined Networking:</b>	An approach to networking that uses software-based controllers or application programming interfaces to communicate with underlying hardware infrastructure and direct traffic on a network.
<b>Smart IoT:</b>	A smart device that has support for Internet connectivity and can interact with other devices over the internet and grant remote access to users for managing the devices based on their needs.
<b>Sniffing Attack:</b>	Theft or interception of data by capturing the network traffic using an application known as a packet sniffer.

# CHAPTER ONE: INTRODUCTION

## 1.1 Background

Traditional network models provide some flexibility in coordination among network devices which must be configured or programmed manually. Any small change in the network can have negative ripple effect on its entire performance. A number of factors make the traditional network management approach outdated namely, growing demands to improve performance of the network, huge volumes of generated data and advanced network designs (Wang, Tao & Lin, 2016). Security is also another concern in all types of networks whether wired or wireless. One of the key advances in networks is the introduction of software programming features to strengthen the network and ensure central coordination of network resources which has resulted in software-defined networking architecture. The architecture compartmentalizes the network into two planes that coordinate together to improve performance of the network. The two planes are the data plane and the control plane (Othmane, Mouad & Redouane, 2017).

According to Zewairi (2017), the data plane is responsible for network data transmission. It is specifically responsible for system configuration, management, and routing table information exchanges. The data plane, also known as the forwarding plane, is in charge of the actual transmission of traffic to the destination network based on the logic of the control plane. The two planes work synchronously and they are distributed throughout the network (Maham et al., 2019). This concept has also been applied in the containment of security threats in both wired (LANs) and wireless (WLANs) networks based on the IP version 4 address. There is a need to extend it to other domains such as Mobile IP version 6 (MIPv6) to contain key security threats such as Sniffing attacks, Distributed Denial of Service (DDoS) attacks, and damage control.

## **1.2 The Concept of Software-defined Networking**

Software-Defined Networking (SDN) is a model that seeks to improve network performance in terms of its control and flexibility under different conditions. Its emergence as a secure, flexible, and well-managed model enables it to provide central network control and management (Bakhshi, 2018). The function is performed through a central controller known as the Software-Defined Networking Controller (SDNc). Once the network has been segregated into control function and data function, it is able to coordinate all the activities such as data transmission, error detection and correction (Zewairi, 2017).

The ease of programming the network using the SDN model makes it exploitable in network security processes such as monitoring, analysis, and response (Cox et al., 2016). The other advantage of the Software-Defined Networking model is that it is adaptable, manageable, cost-effective, and dynamic. Originally, it was used in the wired networks, however, with the widespread adoption of the mobile devices such as smartphones, tablets, smartwatches, laptop computers, and hand-held gaming consoles, it is now used in wireless networks as well (Maham et al., 2019). The wireless networks are applied in all spheres of life such as businesses, homes and even public places. They also make one-to-one mapping of a client and a light virtual access point with a unique and different Basic Service Set Identifier (BSSID) possible.

### **1.1.2 The Concept of Mobile IP version 6 (MIPv6)**

The Mobile IP version 6 supports mobility for Internet Protocol version 6. It allows reserving of one internet address everywhere as well as allowing applications using the same address to maintain transport and upper-layer connections where there is change of location. MIPv6 also allows mobility between homogeneous and heterogeneous media (Samuel, 2018). In wireless networks supported by the MIPv6, each mobile node consists of two IP addresses namely,

home address and care-of address. The home address is usually a permanent Internet Protocol address whose purpose is to identify the mobile node irrespective of its location. On the other hand, the care-of address usually changes at any new point of connection and also provides all the information on the current situation of the mobile node. Any time a mobile node arrives in any network it acquires a care-of address (Tsuguo et al., 2016). The address is used throughout the time the mobile node is in the location of the visited network. The mobile node or device is also able to get the care-off address using the methods of the IP version 6 Neighborhood Discovery which makes both the stateful and stateless auto configuration possible.

The ability of the IP version 6 to support mobility is not available in IP version 4. The mobility functionality is usually complex which raises a number of concerns in regards to security. Mobility in IP version 6 environment uses two types of addresses, the real address which is a typical IPV6 address contained in an extension header and the mobile address which is a temporary address (Samuel, 2018). The characteristics of the networks, therefore, makes the temporary component of a mobile node susceptible to various attacks such as sniffing and DDoS on the home agent. To ward off this challenge, mobility requires special security mechanisms which network administrators must be cognizant of (Tim, 2002).

## **1.2 Research Problem**

Several studies have been conducted on improvement of security using Mobile-Defined Networking model. However, one of the issues still open in the Software-Defined Networks is security exploitation in regards to mobility. Some of the security challenges with Mobile Internet Protocol version 6 (MIPV6) are the sniffing and Distributed Denial of Service (DDoS) attacks. According to Tony (2016), Rene et al (2018), and Maham et al (2019), several studies have been done on Software-Defined Networking as a model to address security challenges. However, these have been confined to wired network architectures. The findings have also

been on IPv4 where the SDN model has been employed to coordinate all decisions of networks through a central authority known as the SDN controller which manages all network connections and associated data flows (Scott et al., 2016). Very few studies have also focused on the comparison of performance between SDN models and traditional models concerning security. With mobility, different devices can move from one access point to the other leading to the introduction of foreign objects in mobile/wireless networks. These can pose security challenges in shared networks where management and control are not done centrally through an SDN controller. The study, therefore, sought to find out how the use of Software-Defined Networking model could be used to improve security in a Mobile Internet Protocol version 6 environment.

### **1.3 Research Objectives**

The following were the research objectives of the study:

- (i) Apply a Software-Defined Networking model to contain Sniffing and DDoS security threats in the Mobile Internet Protocol version 6 (MIPV6).
- (ii) Explore effects of Sniffing and DDoS security threats in the Mobile Internet Protocol version 6 (MIPV6).
- (iii) Determine Software-Defined Networking mechanisms for containing Sniffing and DDoS security threats in the Mobile Internet Protocol version 6 (MIPV6).
- (iv) Show that the Software-Defined Networking model can better contain Sniffing and DDoS security threats in MIPV6 as compared to traditional network models.

### **1.4 Value of the Study**

The discussions of the study would be instrumental to theory development by future researchers and academicians. The concepts and theories advanced in the study would be handy in

augmenting their background knowledge in regards to various thematic areas such as software-defined networking, network service orchestration, and Mobile Internet Protocol version 6 (MIPv6). In addition, the study would also be used as reference point by the researchers and academicians

As a researcher, the study would enhance my understanding of security challenges inherent in the Mobile Internet Protocol version 6 (MIPv6) environment which was an emerging knowledge domain, and how software-defined networking and network service orchestration models could be applied to solve those challenges in wireless networks. To the community, the study would help in solving various network mobility security threats that affect Quality of Service (QoS), traffic overload as well as policies around it. In this way, it would enhance the development of new or improvement of existing commercial products, technology advancements, and or in industrial development that could have a huge economic impact.

### **1.5 Motivation for the Research**

The research study was motivated chiefly by the need to augment the knowledgebase in the area of the Distributed Computing Technology through the application of software-defined networking and security in Mobile Internet Protocol version 6 (MIPv6). This would help foster critical thinking and analytical skills through hands-on learning. Through this study, the researcher would also be able to define his academic, personal, and career path through the acquisition of specialized knowledge leading to the attainment of a master's degree.

## **CHAPTER TWO: LITERATURE REVIEW**

### **2.1 Introduction**

This chapter of the study reviewed the theories, concepts, and empirical aspects of the software-defined networking, and mobile Internet Protocol version 6. It also delved into the exploration of security threats existing in MIPV6 and Software-Defined Networking security containment mechanisms that can be applied to address the threats. Finally, it ended with empirical evidence on how the Software-Defined Networking model has been applied to contain security threats in comparison to the traditional network models.

### **2.2 Theoretical Framework of the Study**

Various studies have advanced several theories regarding how networks behave in terms of performance and security, whether wired or wireless. These theories, among other things, seek to explain various ways of managing or configuring the network components or services either centrally (software-defined) or individually (hardware-defined). These theories are graph theory and network theory.

Over the years, mobile communication networks have massively grown leading to demand for new solutions to emerging problems. The problems are largely related to reduced bandwidth as well as alterations in in various network topologies. In the words of Kanniga and Murugaboopathi (2018), since many users as well as information are stored in other networks, it cannot be guaranteed that all the data will be safe and secure. The data are susceptible to attacks and leakages. Wireless network security, therefore, becomes a core concern that must be addressed by all stakeholders and service providers in order to maintain their relevance in the market. Graph or network theories can assist in solving network problems. It can also be applied in representation of network components using colour codes and in mobile systems to assign problems (Hiroshi et al., 2011).



Several studies such as Lara et al (2016), Zewairi et al (2017), and Samuel (2018) show that both the graph and network theories have been used in both wired and wireless (mobile) networks to explain how network devices are organized, communicate and route traffic among themselves. Suman and Anita (2012) note that “Graph theory can be used to represent communication networks which are collections of terminals, links, and nodes which connect to enable telecommunication between users of the terminals”. The network terminals need to have unique addresses to enable intended recipients to receive the messages. Networks also consist of various components such as terminals, transmission channel, and processors. Terminals refer to network equipment that exist from where the network starts to where it stops while the processors are responsible for controlling data transmission.

### **2.2.1 Relevance of the Graph and Network Theories to the Study**

The graph and network theories concisely fitted into the study of using the Software-Defined Networking model to improve security in the MIPv6. They aided in choosing how the network components were arranged to achieve the network designs adopted for the study. The two network designs adopted various components such as routers to route traffic from one point to the other, switches to segment the network in terms of collision domains, servers to store information, and user terminals to initiate actions such as browsing which trigger information flow in the network and the attack nodes that injected fake packets into the network.

As had been noted, the graph theory informed how the wireless nodes were represented by different colour codes in the network design to distinguish them from one another. This was important because each wireless network component behaved differently and had specific roles to play in coordinating traffic flow in the network. Routers can process the traffic to know its origin and destination based on IP addresses. Switches on the other hand allow networks to

route traffic (messages) using Media Access Control (MAC) address. Adoption of both the graph and network theories, therefore, helped in simplifying the roles of each network component in terms of deciding on which rules or conditions to apply to a network to make it behave in a certain way. Networks behave under certain conditions based on flow table entries and actions that determine signal sources and their routing from one node to another. In this way, attack nodes could be configured to infuse fake packets in the network and also falsify some nodes to allow routing of traffic to unintended nodes. This enabled the network to be easily simulated to enable observation of different behaviours when the network is under attack or not.

## **2.3 Conceptual Framework of the Study**

This section outlined the various concepts underpinning the study such as the software-defined networking, Mobile Internet Protocol version 6 (MIPv6) including security threats in wireless networks. It further compared the SDN model to the traditional models in order to make a conclusion in terms of improvement of security in MIPv6.

### **2.3.1 Software-Defined Networking Model**

Software-Defined Networking has aroused a lot of curiosity in the programming of network designs by simplifying them and making them more innovative unlike the traditional network design approaches (Xenofon, Mahesh & Kimon, 2015). According to Hamid and Hyun (2016), SDN enables network programmability and alters how the networks are designed and managed through abstraction that results in decoupling the data plane from the control plane. As a result, the SDN controller is able to have entire network overview and make decisions, while the hardware consisting of routers and switches becomes responsible for packet forwarding to various destinations by the intervention of the controller through rules.

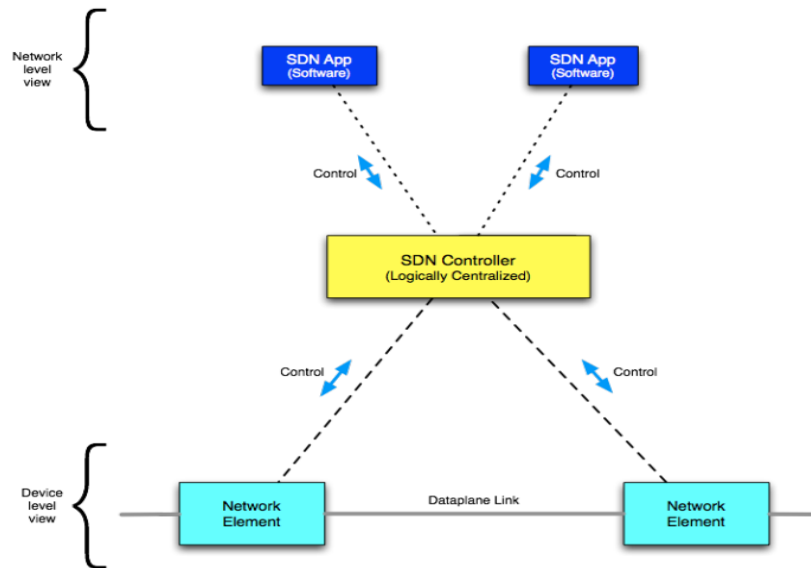


Figure 2.1: Conceptual model of an SDN-controlled network (Adapted from Open Network Foundation 2015)

While early network models that were adopted to bring about a paradigm shift in network design did not yield much, the actual success of the Software-Defined Networking was building on its strong points, while at the same time succeeding in addressing its failures (Xenofon, Mahesh & Kimon, 2015). Hassan and Elaheh (2018) posit that forwarding switches and routers need to be connected directly to the controller for correct operation to achieve desired output from an SDN-controlled network failure to which, they can continue running old policies and leading to inability to receive and forward traffic. As has been noted, Software-Defined Networking decouples the data plane from the control plane which permits running of the network logic on a software controller. The decomposition of the network components and operations have the advantage of simplifying the network management and its programmability leading to resiliency and stability. The SDN is composed of six components namely, the control plane, data plane, northbound interface, management plane, east-west interfaces, and management plane (Othmane, Mouad & Redouane, 2017) which work together to provide control and orchestration of the whole network via application programming interfaces (Kreutz et al., 2015).

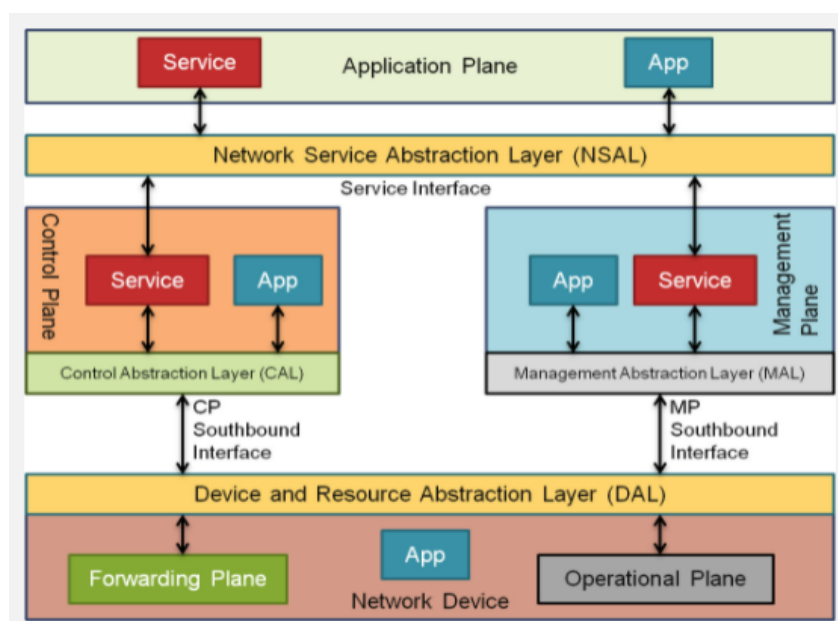


Figure 2.2: The SDN layered architecture (Adapted from the Architecture of IEEE RFC 74262017)

### 2.3.1.2 Software-Defined Networking Security Mechanisms

According to the ONF (2014), a control plane that is logically centralized allows networks to have overall view of all resources. To achieve this architectural design, the Software-Defined Networking employs Network elements that work in synchronicity with the SDN-controller which allows more improved network agility, and operation SDN also allows appliances of security to be easily embedded into the network. Centralization of the Software-Defined Networking offers the advantage of enabling events in the whole network to be integrated, and accumulated, leading to better coherence and accuracy of network operation (Kreutz et al., 2015).

The SDN controllers offer accurate status of network which allow them to detect and act on security incidences easily (Kreutz et al., 2015). Where the SDN is able to detect that it is being hijacked, the controller can push the malicious traffic to an identifier for further analysis and correction. Where the traffic is found to be malicious, the SDN controller is able to filter it off and protect the network from further damage. The automatic detection of the Software-Defined

Networking controller, therefore, protects the traffic integrity making it indispensable in network attack intelligence (Rene, 2018).

### 2.3.2 Mobile IP Version 6

Internet has been believed to consist of static nodes. This, however, has not been the case as new bile and smart components get connected. The number of devices connected to the Interned has increased exponentially leading to challenges in continued use of the IPv4. This situation has been remedied through adoption of the Internet Protocol version 6 (Tim, 2002). Further, out of this, the Mobile IPV6, was made an integration part of the IPV6 to allow mobility of IP based networks in wireless networks. MIPV6 allows mobility of nodes within the internet to roam and reach their intended destinations while still keeping active sessions intact (Tim, 2002).

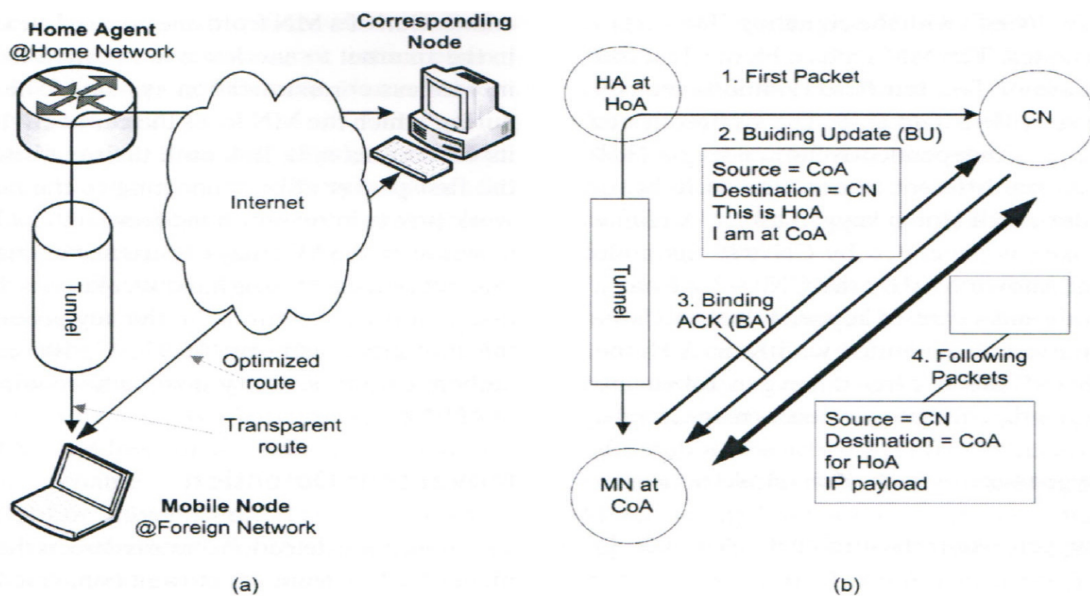


Figure 2.3: MIPV6 Architecture (Adapted from Aura & Roe, 2006)

The design of the Mobile IP v6 allows mobile nodes to move freely while at the same time ensuring that they reach their destinations without causing any distortion to the active sessions (Perkins et al., 2011). During its operation, the MIPV6 employs multiple extensions of the

IPv6 headers principally for signal purposes (Ahmad, Marc & Christian, 2016). Also, the IP address of the mobile node location is able to change as the mobile node changes from one access point to the other.

#### **2.3.4 Security Threats in Mobile IP Version 6 (MIPv6)**

Mobile IP version 6 suffers from several security threats which include unsecure route optimization, spoofing, Distributed Denial of Service, hijacking of sessions, and eavesdropping (Vishwajit & Aumdevi, 2013). When routes are optimized mobile nodes and corresponding nodes are able to communicate effectively without intervention of the home agent. Route optimization occurs where the mobile node receives the message and subsequently updates the corresponding node about its acquired location leading to binding between the two nodes. The binding allows the care-of address and the home address to register in the binding cache. The lack of authentication between MN and CN causes the route optimization to be insecure. An attacker can also hijack existing connections between MN and CN nodes. The attack node can also send traffic attacker can also redirect the packets to random nodes which can disrupt communication between the benign network points. In this case, a new binding message update has to be sent periodically to update the entry of the binding cache to refresh the binding cache (Rene, 2018).

DDoS, as one of the prevalent security threats, manifests itself in many ways. Specifically, it tries to disable access of various computer resources leading to state of starvation (Abdel, 2011). The motive may be unknown; however, it is as a result of efforts of a person or even many people who collaborate through software applications to degrade performance of the network under attack indefinitely or temporarily. Another form of security threat could be eavesdropping which is passive or active information theft. The eavesdropping agent taps into

the network and listens to the traffic. The agent can then tap into the packets on transmission and divert them to unintended destinations (Perkins et al., 2011).

### **2.3.5 Software-Defined (SDN) Networking versus Traditional Network**

#### **Security Threats Containment Mechanisms**

Although there are many similarities between security issues in both Software-Defined Networking models and traditional networks there are several inbuilt functionalities that set the SDN apart. SDN consists of the data plane that is separated from the control plane. The data plan makes it possible to route traffic from one point to the other while the control plane is in charge of making decisions on the network operation. The SDN also enables centralized view of the network making it easier to manage (Kreutz et al., 2015). The other difference between the Software-Defined Networking and the traditional architectures from security perspective is its capability to share and operate a physical network dynamically. The SDN network then is able to secure communication between network components as well as control coordination between applications and tenants through programmed APIs leading to more autonomy in the network operation. This synchronicity leads to mitigation of security threats which is not the case in the traditional networks (Rene., 2018).

In traditional networks, Equipment tends to be monitored and managed in an isolated manner. This makes the network management cumbersome where standard protocols are missing. The Software-Defined Networking, on the other hand, presents the ability to manage and monitor the network in a flexible manner (Kreutz et al., 2015). There could be instances where the control plane may become a bottleneck. However, Abdel (2011) notes that its ability to have an overview of the whole network makes it possible to handle any incidents that are reported more quickly and dynamically.

## 2.4 Empirical Framework

As Vishal et al. (2020) illustrate in diagram 2.4 below, several studies have been conducted around security, trust, and privacy regarding mobile and the Internet of Things (IoT). It also presents analysis and comparison of various works that can be associated with this study. Whereas several studies have focused on mobile or wireless technology, few have endeavoured to capture security challenges and their mitigations in relation to mobility (MIPv6). This technological, as well as security gap, has helped to advance knowledge, particularly about how security can be augmented to cope with rapid development in the wireless field.

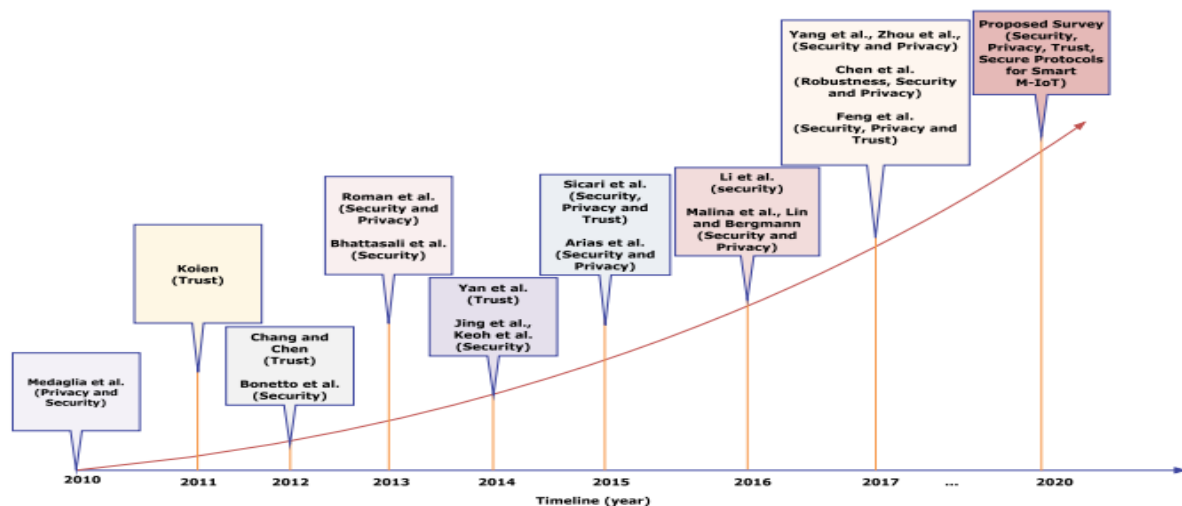


Figure 2.3: Evolution Wireless Security Technologies (Adapted from Trend by Vishal et al, 2020)

Previous studies were largely concentrated around privacy and security in general irrespective of the environment whether wired or wireless. Medaglia et al. (2010) and Koiem (2011) attempt to capture basic considerations for private, secure, and dependable mobile network designs. There is also mention of security concepts to wireless including protocols and frameworks that have been adopted in designing of the such networks (Sicari et al., 2015, Arias et al., 2015 & Yang et al., 2017). Thus, the necessity of further in-depth study on the use of Software-Defined Networking would enable future researchers to have more understanding into how security can be improved in MIPv6.



## **CHAPTER THREE: RESEARCH METHODOLOGY**

### **3.1 Introduction**

The chapter discussed the research approach and tools that were used in the study. It started with research hypotheses, design of the research then data collection, population, and procedures used. It also outlined the statistical techniques used to address issues of validity and reliability of the instruments used for the collection of data, pilot-test, and ethical considerations.

### **3.2 Research Model and Hypothesis Formulation**

In this research, dependent variables were drawn from the software-defined networking model while independent variables were drawn from the mobility environment (MIPv6), based on the DDoS and Sniffing security threats under consideration. Since the three interrelated perspectives were supported in the use of the software-defined networking model to contain the two security threats in MIPv6, they were adopted as follows: the software-defined networking model perspective (which dealt with how wireless networking components are programmed and coordinated to achieve synchronicity in managing network resources); device mobility perspective (the wireless network components such as laptops, tablets, iPads, and mobile phones) move from one access point to the next, meaning that they acquire and re-acquire IP addresses from one location to the next, and traditional network model perspective (the wireless network devices are managed independently without any programmability or central coordinating components).

The model of the research, therefore, allowed the researcher to validate the hypotheses outlined below:

H0: Use of the Software-Defined Networking has a positive effect on the Distributed Denial of Service and Sniffing attacks on MIPv6.

H1: Device Mobility has a negative effect on the Distributed Denial of Service and Sniffing attacks on MIPv6.

H1: Traditional Network models have a negative effect on the Distributed Denial of Service and Sniffing attacks on MIPv6.

### **3.3 Research Design**

The study used an experimental research design. Experimental research design sought to find out the cause-and-effect relationship using direct manipulation of both independent variable and extraneous variable. As noted by Uma and Wiley (2016, p. 97), experiments more often than not relate to hypothetical deductions in the research being conducted. The reason for carrying out experiments is simply to investigate the causal relationships existing between variables. Where an experiment is conducted, it is up to the researcher to manipulate the independent variable to investigate what effect the manipulation have on the dependent variable then give comparative results to fit the study. Usually, research designs may also refer to blueprints or plans that are used to collect, measure, and analyze data that are created to respond to research questions (Tahira, 2019).

Specifically, a lab experimental design was adopted for the research. There the cause-effect relationship exists between a dependent and independent variable needs to be established, the other variables that may alter the relationship must be controlled in a tight manner (Alan & Emma, 2011). It is also important that any effects on any other variables affecting the dependent variable be accounted for to help investigate the effect of the independent variable

on the dependent variables. The manipulation or control of the dependent variable can only be done in a controlled setting such as a laboratory. The research design, therefore, fitted the study since it sought to find out why software-defined networking models can better address DDoS and Sniffing attacks in MIPv6 as compared to traditional wireless network models.

### **3.4. The Population and Sampling Methods**

#### **3.4.1 Target Population**

Study population refer to the objects that are under investigation. The population has to be specific or specified. The population usually means all objects or items that a researcher wants to investigate (Uma, 2016). Hence in this study, the population comprised of all the objects that were assembled into a wireless topology for testing purposes. The topology made it easy to simulate two types of wireless networks, that is, network topology without SDN and network topology with SDN. The two wireless network topologies consisted of routers, servers, normal client nodes, and DDoS attack nodes. The attacking node was the independent variable that controlled the behaviour of control routers (dependent variables) in the study.

In the case of the software-defined network model, an SDN controller (SDNc) was included to centrally manage the network through software programming. In this case, all the network components (servers, routers, and clients were programmed, coordinated, and administered centrally unlike in the traditional topology (without SDN) where network components were controlled independently.

#### **3.4.2 Population Sample**

The target population consisted of network objects that were organized into two topologies to be tested in a controlled manner. The components consisted of servers, routers, mobile client nodes such as laptops, mobile phones, tablets, and iPads, and an attack node. In the simulated

environment, the nodes were configured to allow for the triggering of data packets from one node (access point) to the other. The routers used their routing tables to tell if the packets triggered were genuine or fake. The client nodes referred to various applications that used the network to conduct various activities such as surfing and reading mails, among others. Interfaces consisted of simulated traffic lines between nodes that acted as paths for data packets between nodes.

### 3.4.3 Sampling Technique Used

The study adopted judgmental method of sampling which was found to be ideal due to the fact that a reasonable quantity of objects could be used as primary source of data. The technique was also premised on the need to consider the number of components that would be used to simulate the two environments chosen to investigate the use of the SDN model in containing DDoS and Sniffing attacks in MIPv6. A reasonable number of components was, therefore, picked to ensure that the two designed networks were able to operate and give desired results.

To determine the size of the population, the researcher used the following formula:

$$n = \frac{Z^2 \alpha^2 p(1-p)}{d^2} \quad (\text{Kothari, 2006})$$

Here,

N denoted the size of the sample,

Z $\alpha$  was chosen to be the normal standard deviation at where the confidence level was needed,

d in this case referred statistical significance level set,

p denoted the estimated population that was targeted in terms of the characteristics that were to be measured,

Z $\alpha$  was a value that was chosen in a way that the standard normal variable could exceed

$(1-\alpha)/2$ . The value picked for the  $\alpha$  level was obtainable from a table that gave the value of Z as the normal distribution standard.

With 95% as the level of confidence, the value of  $Z\alpha$  became 1.96. This was based on the fact that there was no available estimation for the available targeted population proportion. Therefore, 30% sufficed (Mugenda & Mugenda, 2003). That is, p was taken as 20%, d as 0.05% at the level where the desired accuracy was 0.03.

From the above, the population sample size n became:

$$n = \frac{1.962 * 0.5 (1 - 0.5)}{(0.052)}$$

$$n = 33$$

therefore, 33 was the population size used, taking into consideration the number of network components that were organized to achieve the two simulated network designs.

### **3.5 Methodology**

As had been noted, the study investigated how SDN could be used to address Sniffing and DDoS attacks in MIPv6. The questions were answered were based on the effects of the security threats in the MIPv6 environment. Specifically, sniffing attacks, DDoS attacks, and damage control scenarios were considered. To achieve this, several steps were considered namely, deciding on the number of network components, process flow, wireless network design, and implementation as outlined below.

### 3.5.1 The Network Components

Two network topologies were considered: network topology without the SDN and network topology with the SDN. The network design without the SDN consisted of 16 components while the network design with the SDN consisted of 17 components which included the SDN Controller. The components were then organized into two simulated setups to gather the needed information. At a minimum, the table below shows the network components that were assembled to come up with the two environments:

Table 3.1: Summary of Network Components

SNO	COMPONENT NAME	NUMBER	IP ADDRESS/ IDENTITY
1.	Router 1	2	2901
2.	Router 2	2	2901
3.	Router 3	2	2901
4.	Router 4	2	2901
5.	Router 5	2	2901
6.	SDN Controller	1	SDN
7.	Switch 1	2	2960-24TT
8.	Switch 2	2	2960-24TT
9.	DDoS Attack Node	2	192.168.1.160
10.	Sniffer Node	2	Sniffer
11.	User Terminal 1	2	C1
12.	User Terminal 2	2	C2
13.	User Terminal 3	2	C3
14.	User Terminal 4	2	C4
15.	Server 1	2	192.168.1.178
16.	Serv 2	2	192.168.1.194
17.	Server 3	2	192.168.1.21

### 3.5.2 The Process Flow Diagram

Figure 3.1 below shows the Process Flow Diagram that was adopted to illustrate the behaviour of the two networks. Here the router received the packet and checked its routing table to

confirm the origin. If the entry was found in the routing table of the router, the packet was forwarded to the destination. However, where the packet entry was not found in the routing table, the SDN controller took over. In the event that there was high packet volume from the router, the SDN switched off the router. Sometimes, the SDN controller could not determine unusual behaviour, in which case, advanced cryptographic mechanisms (HashMap) were used by the controller to further confirm address of the packets. In case the address not found, the packets were discarded. Otherwise, the correct entry was updated in the flow table.

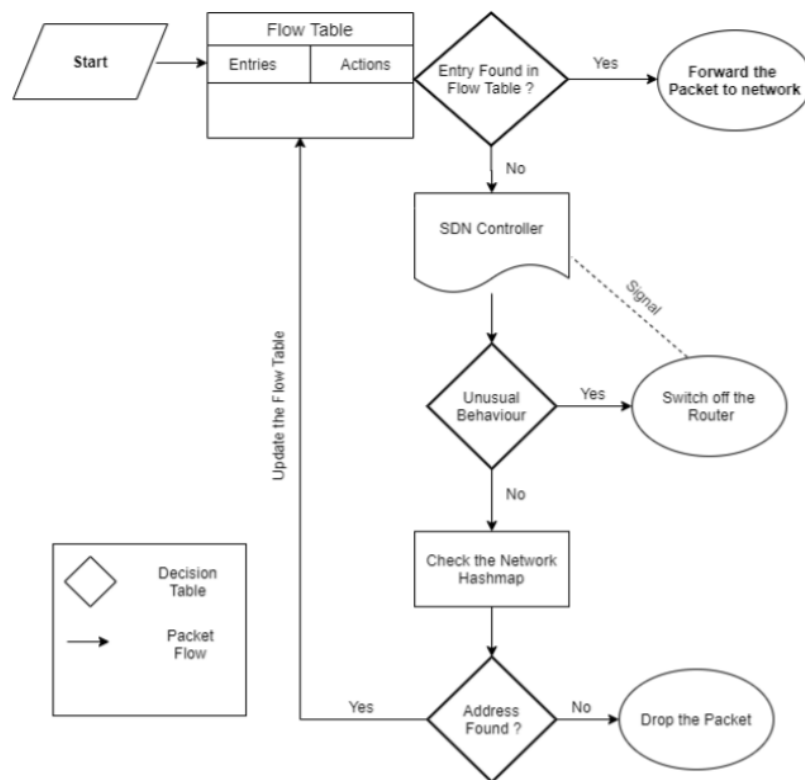


Figure 3.1: Flow Diagram of Proposed Process Flow (Adapted from Methodology Approach of Ajay, 2020)

### 3.5.3 Design and Implementation of the Wireless Network

The network was designed using various components such as routers, client terminals, server and switches. The components were organized into a total of 14 nodes. Two nodes out of these were designated as attacker nodes namely, sniffer and DDoS. The sniffer node would

compromise the R5 and divert part of the benign packets to itself or to R4 leading to reduction of the number of the packets flowing in the network from the origin, C3, to destination, S2. The DDoS node also served as an attacker node that injected fake packets into the network by compromising R3 or at the same time diverting the genuine packets to R4 and then to S4. The nodes in the network design were configured with IP addresses to enable routing of traffic within the network. Two types of networks were designed as discussed below:

### 3.5.3.1 Network Topology without SDN

Here, the network components were connected and configured to function in a legacy manner. This meant that the nodes, especially the routers and switches were supposed to use the rules or protocols configured in them to react to any unusual behaviours caused by the attacker nodes in the network. The traditional networks usually employ inbuilt mechanisms to recover in the event of attacks. This topology is shown in Figure 3.2 below.

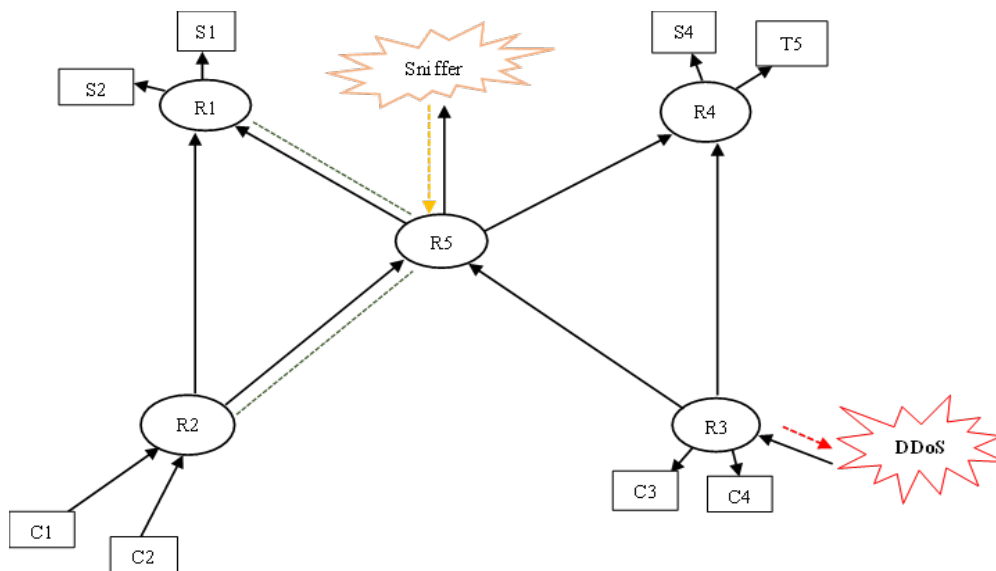


Figure 3.2: Network Topology without SDN

Traditionally, the network mainly relies on the physical infrastructure which includes routers, switches, and servers to generate packets, route them and employ available mechanisms to



recover in the event of attacks. In this case, target of a network was programmed to route traffic within the network. To demonstrate this, both DDoS and sniffing attacks were configured. The traditional network was then subjected to the two attacks which were intentional. The two scenarios were analyzed as indicated below:

#### **Scenario One: Sniffing Attack**

In this scenario, the hacker tried to capture and analyze network communication information as follows. Client C3 generated the packets and sent them to Router R3. When the packets reached the router, the source and destination IP addresses were extracted from the packets. The router searched its flow table and confirmed that the packet was supposed to be routed to R5. R5 then forwarded the packets to the final destination which was R1. However, in the event that the network was under attack, the sniffing node impersonated itself as S4 which subsequently rerouted the packets from R5 to R4 and then to S4. This was the case because there was no SDN controller which was intelligent enough to stop the unusual behaviour.

#### **Scenario Two: DDoS Attack**

In this investigation, the DDoS attack directed large traffic was injected into the network by the DDoS attack node. Consequently, R5 was not able to handle the large number of packets that were coming from R3 as a result of the DDoS node spamming the network. In this case, C3 and C4 could not transmit packets to the network which disabled all the services of the network.

### **3.5.3.2 Network Topology with SDN**

Here, the Software-Defined Networking controller was incorporated into the network to provide additional protective layer in the event of an attack. The SDN controller was

programmed to provide capabilities of both the data plane and control plane. Three scenarios were analyzed as below:

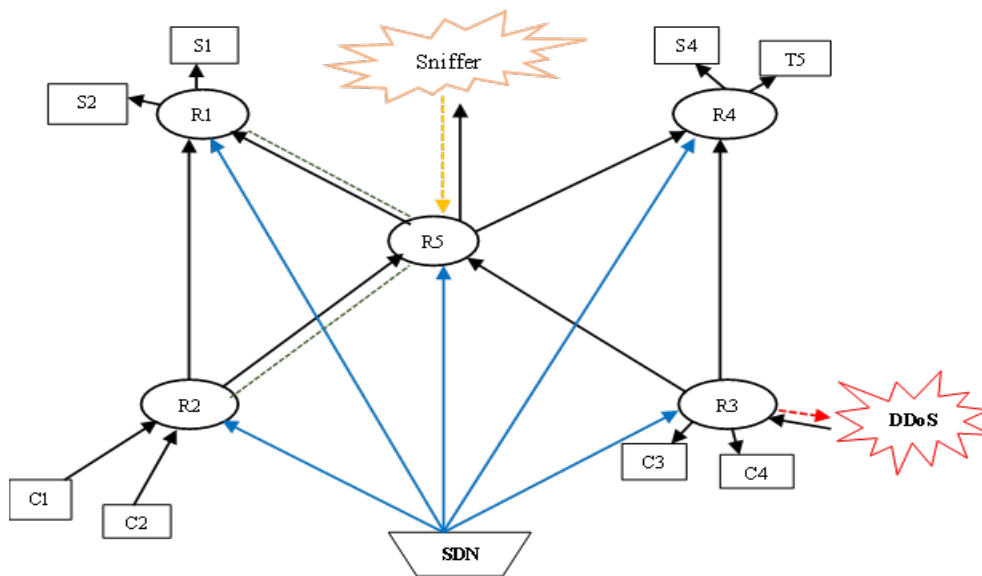


Figure 3.3: Network Design with SDN

### Scenario One: Sniffing Attack

The same scenario without SDN was considered here. Client C3 generated the packets that were sent to Router R3. When the packets reached the router, it extracted the IP address to ascertain origin and destination of the packets. This was possible because each router contained their own packet flow information. In this particular scenario, C3 originated the packets to R3 which then forwarded the packets to R5. The attacker node attempted to divert the packets to R4 instead of R1 and then to S2. However, since there was SDN controller which had an overview of the entire network, this could not happen. Hence, all the packets from C3 were routed to S2.

### Scenario Two: DDoS Attack

The scenario was repeated as in the case of the network without the SDN where C3 originated packets to R3 then to R5 all the way to S2. During this process, the DDoS attack node generated huge amount of data to R3 which used its routing table to confirm identity of the packets. The

packets whose IP addresses matched the entries in the flow tables were routed to R5 which those that were not found were dropped by the SDN. The SDN was, therefore, able to protect the network from the fake packets generated by the attacker node. In the same vein, the huge number of the packets generated by the DDoS node overwhelmed R3 which led to it being disabled. However, since the SDN had the entire view of the network, it was able to reroute the genuine packets sent by C3 through R2 to R5 which then found their ways to S2.

### **Scenario 3: Damage Control**

Damage control is where links between two or more network nodes are damaged and so cannot allow traffic to be routed from one point to the other. To demonstrate this, packets were generated from Client C3 and forwarded to Router R3. Router R3 checked its flow table and confirmed that the packets were destined to Router R5. Since the link between Router R3 and Router R5 was damaged, the SDN controller took over and rerouted the traffic via Router R2 which forwarded the packets to Router R1 up to Server S2. In this case, the network was able to function normally even if the link between R3 and R5 was damaged leading to a disconnection between the two network components.

### **3.5.4 Topology Implementation Tool**

To implement the proposed architecture, Cisco Packet Tracer was used due to its popularity in simulating the client, server, and router classes in the virtual working environment. The Cisco Packet Tracer is a tool that can be used to simulate network topologies without the need for a hardware or preexisting network (Andrea, 2018). The tool offers many functionalities such as command line (CLI) which enables one to interact with the tool to run various commands and get the results displayed. Due to its popularity in simulating network designs and using the environment to interact with various commands, the tool enabled the researcher to simulate the two network topologies and investigate their performance under the 2 scenarios.

## **3.6 Data Collection**

### **3.6.1 Primary Data Collection**

The research used observation and recording as primary data collection instruments. The information obtained through the observation and recording is similar to that obtained by an interview (Burns & Grove, 1993, p. 368). Two sets of primary data were collected. One was gleaned from a simulated wireless network without an SDN where packets were triggered to move in the network from one node (router) to the next based on routing information contained in the Routing Tables. As the packets moved within the network, a DDoS attack was injected into the network to sniff the packets or introduce fake packets into the network, and observations were made on what happened to the destination router nodes. The observation obtained from the network log was also recorded in a table for analysis.

In the SDN simulated environment, the same topology was used. However, a software-defined networking controller (SDNc) was included to manage the network centrally. In this case, the activities of the attack node (DDoS) were controlled by checking the validity of the packets originating from the attack node in the Routing table. Where the packet headers' information did not match the ones stored in the routing tables, such packets were dropped. In an SDN-controlled network, suspicious activities were therefore prevented leading to the elimination of the security threats. The information obtained from the network log was also entered in a table for analysis.

In both scenarios, attack packets (sniffing and DDoS) were introduced into the network from the attack node and flow of the packets per second was recorded. The following four tables were the results of the observation made from both networks without SDN and networks with SDN simulated environments.

### Scenario One: Sniffing Attack Without SDN

Table 3.2: Flow of Packets under Sniffing Attack without SDN

<b>Time (seconds)</b>	0.0	1.5	2.5	3.5	4.5	5.5	6.5	7.5	8.5	9.5	10.5	11.5	12.5	13.5	14.5	15.5
<b>Flow of Packets</b>	0	10	25	42	68	102	99	120	81	76	50	53	55	53	52	52

### Scenario Two: Sniffing Attack With SDN

Table 3.3: Flow of Packets under Sniffing Attack with SDN

<b>Time (seconds)</b>	0.0	1.5	2.5	3.5	4.5	5.5	6.5	7.5	8.5	9.5	10.5	11.5	12.5	13.5	14.5	15.5
<b>Flow of Packets</b>	0	5	24	28	33	34	33	32	22	18	17	16	8.4	8.3	8.4	8.5

### Scenario Three: DDoS Attack Without SDN

Table 3.4: Flow of Packets under DDoS Attack without SDN

<b>me (seconds)</b>	0	1	2	3	4	5	6	7	8	9	11	12	13	14	15	16
<b>Flow of Packets</b>	0	16	44	28	26	27	99	128	106	89	80	78	74	74	74	71

### Scenario Four: DDoS Attack With SDN

Table 3.5: Flow of Packets under DDoS Attack with SDN

<b>Time (seconds)</b>	0.0	1.5	2.5	3.5	4.5	5.5	6.5	7.5	8.5	9.5	10.5	11.5	12.5	13.5	14.5	15.5
<b>Flow of Packets</b>	0	12	26	26	25	25	26	18	13	12	13	12	11	12	12	11

## 3.6.2 Secondary Data Collection

The secondary research data were gleaned from existing sources articles in academic journals, published books, unpublished reports, and internet sources on software-defined networking,

network security, and MIPv6 operation. Further, content analysis techniques were used to analyze the data collected and to draw conclusions.

### **3.7 Data Analysis**

This research study used both quantitative and qualitative data analysis techniques. Data analysis encompasses the process through which researchers mine and arrange data to gain more understanding of the data and also demonstrate their knowledge they have gained from other people. Data analysis also deals with arranging and separating data into various categories for ease of understanding. The researcher, therefore, adopted various approaches to analyse outputs from the observations made.

Presentation of data entailed using tabular formats to capture the source data that were collected from the observations made during the controlled experiments. The tables were five in total as per the number of the scenarios that were analyzed. Further analysis was done using Python which made it easier to translate the tabulated data into graphs that showed various trends of the number of packets that were transmitted by the network per unit seconds for all the scenarios analyzed above.

### **3.8 Reliability and Validity**

The data obtained were analyzed statistically to ensure that they were reliable and valid. Secondary data that were qualitative in nature were analyzed using content analysis which allowed inferences and characteristics of various trends to be made. Overall, the process of performing reliability and validation processes on data were to ensure that they were in the correct format and form.

### **3.9 Ethical Considerations**

Ethical considerations ensured that the study was conducted according to set of standards that guide researches against fabrication and fraud, and plagiarism. It also ensures that writing and publishing ethics are adhered to. Based on the above argument drawn from the findings of Akaranga and Makau (2016), the following ethical considerations were applied in the research study:

#### **Fabrication and Falsification or fraud**

The researcher ensured that the study was devoid of any form of falsification or fabrication that would lead to manipulation or faking of data or the process involved in the study. This would have led to violation of the primary objective of the research. The outcomes of the study, therefore, were aligned to the research standards and views held by other researchers or scholars.

#### **Plagiarism**

The study ensured that the work produced was original and free from any sources of data or processes that were manipulated. This was applied to the entire document as a way of preserving the originality of the work.

#### **Writing and Publishing Ethics**

Like any other academic writing, the findings of the research were published in peer-reviewed journals and repository as part of research development in all higher learning institutions. To meet these criteria for publishing, the researcher ensured that the work was original and made significant knowledge contributions to the areas where the scholars were interested in.

### 3.10 Summary of Methodology

Below shows the methodology that was used to address the various objectives of the study:

Table 6: Summary of Methodology

SNO	RESEARCH OBJECTIVES	METHODOLOGY
1.	Apply a software-Defined Networking model to address security threats in MIPv6.	For this objective, the researcher used observation, and recording of findings, qualitative and quantitative data analysis, presentation, and derivation of conclusions.
2.	Explore security challenges in MIPv6.	Secondary data collection methods adopted. This included use of content analysis on articles in academic journals, published books, unpublished reports, and internet sources on software-defined networking, network security, and MIPv6.
3.	Determine Software-Defined Networking security containment mechanisms in MIPv6.	
4.	Show that the Software-Defined Networking model can better manage security threats in MIPv6 as compared to traditional network models.	Qualitative, Quantitative, and Comparative analyses of findings from the two models (SDN and Traditional models) were used.



# **CHAPTER FOUR: DATA ANALYSIS, FINDINGS, AND DISCUSSION**

## **4.1 Introduction**

This area of the study dealt with analysis of the data, presentation of results and then concluded with a discussion of the findings. The primary data that were collected by observation as well as those collected from secondary sources were analyzed and presented according to the objectives of the study. It started with an overview of the title of the study which was, “Use of Software-Defined Networking Model to improve security in the MIPv6”. It then delved into the application of the Software-Defined Networking model to address security threats in MIPv6, exploration of security challenges in MIPv6, determination of Software-Defined Networking mechanisms in MIPv6, and demonstration that the Software-Defined Networking can better manage security threats in MIPv6 as compared to traditional network models. The chapter concluded with discussions of the findings.

## **4.2 Data Analysis**

### **Scenario One: Sniffing Attack without SDN**

The number of packet flows per unit second was plotted to produce a line graph between zero second and the 16<sup>th</sup> second. The graph showed that there was an incline in packet numbers between zero and the 7<sup>th</sup> second. Thereafter, the graph started declining up to about the 11<sup>th</sup> second and then plateaued as shown in figure 4.1 below.

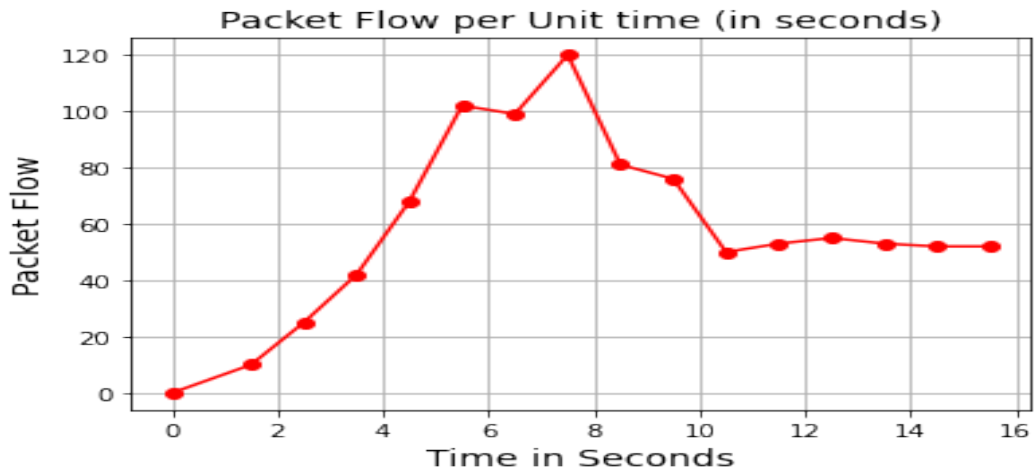


Figure 4.1: Sniffing Attack without SDN

### Scenario Two: Sniffing Attack with SDN

Under this scenario, packet flows per unit second number was plotted to show the behaviour of the network under sniffing attack with the SDN. The traffic peaked at about 33 packets and then reduced before plateauing at about 8 packets per unit second. This showed that when an SDN controller was incorporated into the network, it behaved normally by eliminating the unusual behaviour of the attacker node.

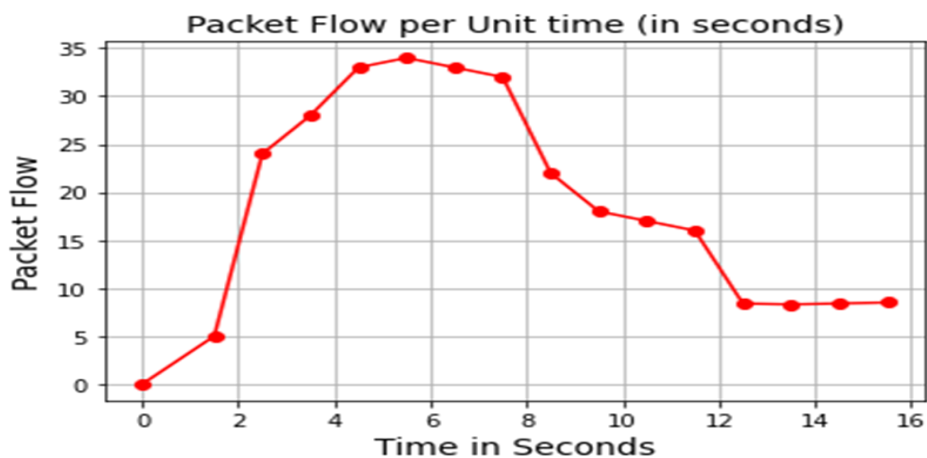


Figure 4.2: Sniffing Attack with SDN

### Scenario Three: DDoS Attack without SDN

A graph was plotted from the data collected under the DDoS attack without the SDN. The graph showed a steep incline in the number of packet flows per unit second up to the 8<sup>th</sup> second at about 126 packet count. The traffic then reduced and plateaued at around 65 packets per second from the 11<sup>th</sup> second onwards. The traffic flow was, therefore, unusual as a result of the hacker node activities.

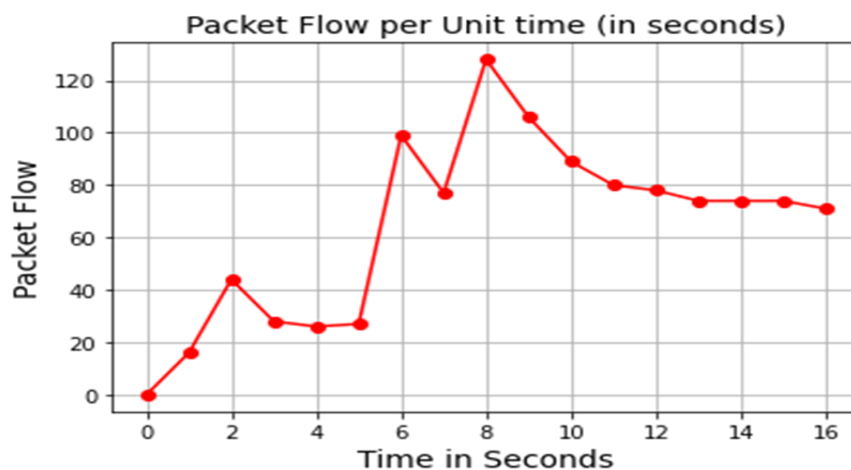


Figure 4.3: Sniffing Attack without SDN

### Scenario Four: DDoS Attack with SDN

Here, a graph was plotted for the packet flow per unit second using the data collected from the DDoS attack with the SDN controller incorporated. The graph clearly showed that the traffic flow was lower than that of the DDoS attack without the SDN. In this case, the SDN prevented the network from the DDoS attack demonstrating that an SDN model can better contain network security challenges as compared to the traditional models.

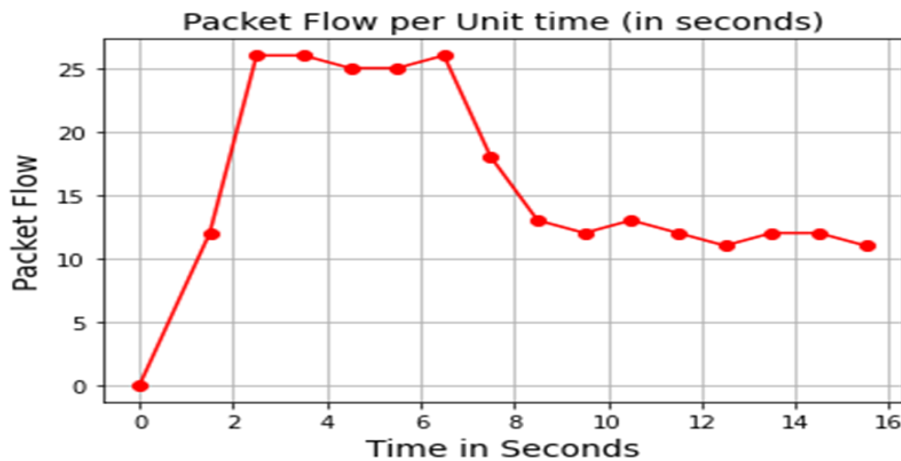


Figure 4.4: DDoS attack with SDN

### 4.3 Research Findings

#### 4.3.1 Application of SDN to address Sniffing and DDoS Attacks in MIPv6

From the simulated environment with the SDN topology, all the network components such as R1, R2, R3, R4, and R5 were connected to the central controller that was simulated with SDN capabilities. In particular, the R3 which was connected to the DDoS attack node had its state registered by the controller. The traditional topology, on the other hand, it was noted that each network component (router) could only rely on the routing decisions in its table to determine the originating and destination IP addresses of the packets coming to and leaving it.

The study established that the SDN model could be used in containing both sniffing and DDoS attacks in Mobile Internet Protocol version 6. The SDN model presented a view of the entire network components stored in its HashMap hence it was able to tell where there were faults or fake packets. If any wireless network node router was compromised, the SDN controller used its advanced routing table (HashMap) to reroute the packets to the intended destination. In the case of a sniffing attack where Client C3 generated the packets and sent them to Router R3, the router was able to forward the packets to R5 which was able to tell from its routing table that the packets were destined for R1 and finally to Server S2 without being diverted by the attack

node to Router R4. This was because the SDN had an overall view of the network, hence it was able to protect it from the sniffing attack.

For the Distributed Denial of Service attack, the SDN controller was able to detect the large traffic that the network kept on generating. In this case, the fake packets that were being generated and sent to router R2 were easily detected by the SDN controller. Where there was unusual behaviour, the SDN was able to disable the respective router. On the other hand, the study established that where there was unusual behaviour, the SDN would check the network HashMap address and refresh all the routers' routing tables leading to containment of the DDoS threats.

#### **4.3.2 Security Challenges in MIPv6**

The study established that, like traditional wireless network models, software-defined networking wireless network models were faced with the same security threats such as sniffing attack and the DDOS attack. It was observable that the attacker node was able to introduce a large number of packets into the network. In addition, it was noted that the attack node could further compromise various network components by spoofing their IP addresses leading to the packets being diverted from intended destinations, say S2 in this case to R4 and then to S4.

In the traditional wireless network topology, the study showed that sometimes the attacker node could compromise the network components which can result into the node diverting the traffic from intended destinations to unintended nodes. In Table 3.2 and Table 3.3 above, the number packets in unit second was much higher for the two attacks. In addition, the attack node could compromise the links between nodes in the network disabling them from having established and dedicated paths to forward the packets. In both cases, however, it was observed that when an SDN controller was introduced in the wireless network, the two main security threats

mentioned above were reduced considerably. This finding, therefore, demonstrated that Mobile Internet Protocol version 6 (MIPv6) environments were faced with security challenges. And these could be addressed through the use of software-defined networking models.

### **4.3.3 SDN Security Threats Containment Mechanisms in MIPv6**

The study established that a software-defined networking model has inbuilt mechanisms that enable them to contain security threats in Mobile Internet Protocol version 6 environments. The mechanisms achieve their effectiveness because of the programmability nature of the SDN. From the architecture of the software-defined networking shown in Figure 2.2 above, the study concurred that the SDN model employs the following mechanisms to contain security threats in the MIPv6 setup.

#### **Use of HashMap**

The study showed that if unusual behaviour was not found and a particular node (router compromised), the SDN was able to check the HashMap and update all the routing tables of the routers with the correct packet IP addresses. However, in the event that the addresses were not found in the routing tables, the packets were dropped. The SDN was, therefore, able to prevent the network from the DDoS attack.

#### **Knowledge of all Network Components**

The study established that the software-defined networking could be configured to connect to all the network components responsible for routing traffic in the network. From Figure 3.3: Network Topology with SDN, it is observable that the SDN Controller connected directly to all the routers. That way, the SDN Controller had an overall status update of all the network components and could intervene whenever any of the components was compromised.

### **Disabling of Compromised Network Components**

The findings showed that the SDN was able to disable R2 which was under the DDoS attack and save the network from the fake traffic from being directed to the unintended destination, R4 in this case. Again, the effect of the attacker node led to the damage of the link between R2 and R5. However, the network could still route the traffic normally through the SDN controller via Router R2 where the packets were forwarded to Router R1 up to Server S2. In this case, the network was able to function normally even if the link was damaged leading to a disconnection between network components.

### **Segregation of the Data Plane and the Control Plane**

The SDN architecture showed that the data plan and the control plan were distinct from one another in terms of their designs and functions. The study concurred with this theory by establishing that it was possible to configure controls in the SDN setup to handle routing decisions and traffic routing decisions separately. This ensured faster decision-making and recovery of the network from both sniffing and DDoS attacks.

### **Load Balancing among Network Routes**

The study demonstrated that it is possible to configure various metrics in the SDN network such as load balancing and shortest route first to ensure efficient use of network resources. To confirm this, the traffic originating from Router R2 was flown directly to Router R1. However, because of load balancing, the traffic was routed via Router R5. It was concluded that SDN used load balancing concepts to create routing efficiency in the networks.

### **4.3.4 SDN as a better Model to Improve Security in MIPV6**

To demonstrate that a software-defined networking model could better manage security threats in MIPV6 as compared to traditional network models, the four sets of data collected from the

two simulated environments were combined into a single graph. The two scenarios analyzed were sniffing attacks without the SDN combined with the sniffing attack with the SDN and DDoS attacks without the SDN combined with the DDoS attack with the SDN. The resulting graph was as illustrated below.

**Scenario One: Comparison between Sniffing Attack without SDN and Sniffing Attack with SDN**

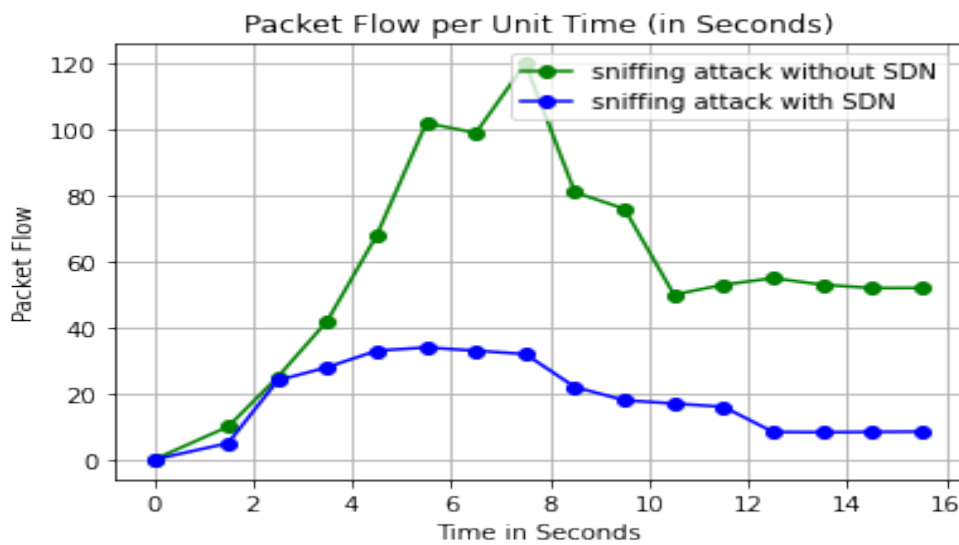


Figure 4.5: Packet flow for both sniffing attack without the SDN and sniffing attack with the SDN

Here a two-line graph for sniffing attack without the SDN and sniffing attack with the SDN was plotted as shown below. It was observed that the simulated topology without the SDN registered a much higher number of packet flows per unit second as compared to the simulated topology with the SDN model. This was because under the topology without the SDN, the R3 was compromised making the network unable to control the flow of benign traffic from C3 to S2. The finding shows that the activity of the hacker node could not be stopped as there was no other component that knew that the network had been compromised. Since the hacker node impersonated itself as server S4, all the traffic to S2 was transmitted to S4 by R4.



## Scenario Two: Comparison between DDoS attacks without SDN and DDoS attacks with SDN

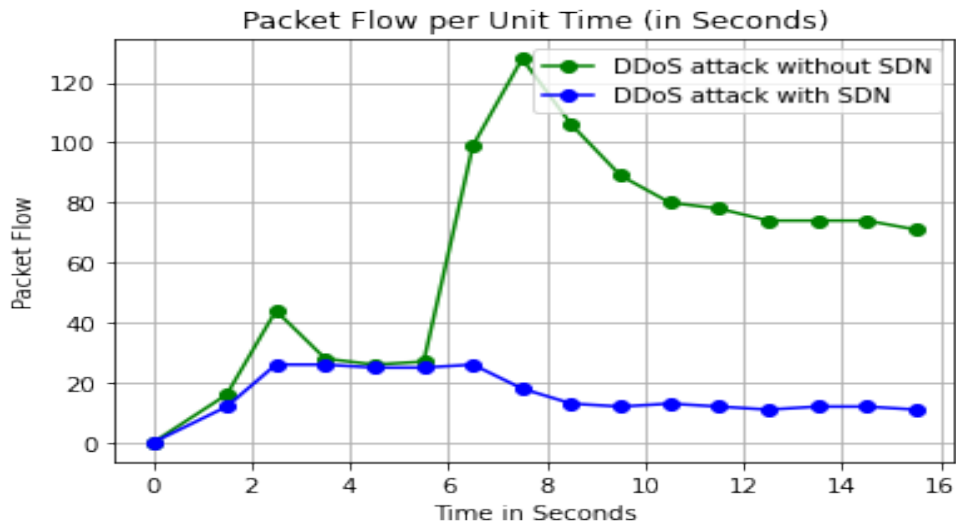


Figure 4.6: Packet flow for both DDoS attacks without the SDN and DDoS attacks with the SDN

Here the findings from the DDoS attack without the SDN and the DDoS attack with the SDN were combined for comparative analysis. From the resulting graph, it was observable that the flow of packets per unit second was higher in the topology without the SDN as compared to the DDoS note with the SDN. This was because the attacker node redirected huge amounts of traffic to the servers, routers, and the other network components rendering the webserver inoperable. The attacker node generated large fake traffic and directed to R3 which were either forwarded in the network or led to crushing of the router.

The observed low amount of traffic in the DDoS attack with the SDN in place was because the controller was able to detect the spams from R3 and subsequently disabled it leading to normal behaviour of the network. Where this was not possible, the HashMap was used to perform more advanced analysis on the packets to determine the correct IP addresses. If the addresses were found, the routing tables were updated accordingly. However, if no addresses were found, the packets were discarded.

## 4.5 Discussion of Findings

Discussion of findings started with testing the three hypotheses. In the first case, the findings showed that the Software-Defined Networking model improved security in MIPv6 by providing alternative routes to traffic. It was also able to isolate the network node that had been compromised by the attack node. This led to the acceptance of the hypothesis. Therefore, the conclusion reached was that sniffing and DDoS attacks could be contained through the use of a Software-Defined Networking model.

In the second case, it was observed that mobile devices changed locations, but retain their identities such as Home Address (HoA). Devices in any mobile or wireless setup could be configured to continue communicating among themselves despite changing their locations. The setup could only be affected if attacker nodes accessed it and injected fake packets into the network which could lead to network devices being compromised. However, with the inclusion of the Software-Defined Networking controller, this was not the case as it had inbuilt functionalities to contain both the sniffing and DDoS attacks. Therefore, this led to the rejection of the hypothesis that device mobility has a negative effect on the DDoS attack as well as sniffing attack in MIPv6.

Secondly, it was observed that in traditional models where there were no Software-Defined Networking controllers, such networks are prone to sniffing and DDoS attacks. In this case, network components such as routers and switches were easily cloned by attacker nodes leading to the rerouting of benign packets from intended destinations. The finding agreed with the hypothesis that traditional network models could be compromised by both the DDoS and sniffing attacks. In the event of an attack, the SDN controller could disable the compromised components of the network. Hence saving the network from more negative effects.

The study further showed that just like the traditional network models, SDN networks also faced several security challenges such as sniffing attacks, DDoS attacks, and link damage. However, in traditional models, the security challenges were more pronounced. Hence the need to employ models such as SDN to mitigate their effects or eliminate them. This concurred with the findings from Vishwajit & Aumdevi, (2013) which confirmed that Mobile IP version 6 suffers from several security threats including unsecure route optimization, connection hijacking, Denial-of-Service (DOS), and eavesdropping among others.

The research concurred with the graph and the network theories that underpinned the study. As studies such as Lara et al (2016), Zewairi et al (2017), and Samuel (2018) show, both the graph and network theories have been used in both wired and wireless (mobile) networks to explain how network devices are organized, communicate and route traffic among themselves. For example, Suman and Anita (2012), agreed that the graph theory has been widely applied in telecommunication to show how terminals, links and nodes are arranged. The advantages of the SDN model in managing MIPv6 security challenges should, therefore, encourage the adoption of such models in designing and operationalizing wireless networks in general.

# CHAPTER FIVE: SUMMARY, CONCLUSION, AND RECOMMENDATIONS

## 5.1 Introduction

Here, the researcher considered the summary of the findings, conclusion on the study, study limitations, and suggested areas for more studies. Under the summary of findings, the four objectives were discussed. This was followed by the overall deduction on the study. Limitations, on the other hand, dealt with the aspects that the study could not conclusively validate that were suggested for further research.

## 5.2 Summary of Findings

*Objective 1: Apply the Software-Defined Networking model to contain Sniffing and DDoS security threats in Mobile Protocol version 6 (MIPv6)*

The study established that the SDN model could be used to contain sniffing and DDoS attacks in MIPv6. By programming an SDN controller into the network, it became more resilient and was able to have the whole view of the network. In the case of a sniffing attack, the SDN controller stopped the sniffing node from diverting the benign packets to R4 and then to S4. On the other hand, it was expected that under the DDoS attack, the fake packets from the attacker node would overwhelm R3 and access the rest of the network leading to a high amount of traffic. However, the SDN controller contained this by disabling R3. Similarly, if the link between R3 and R5 was compromised, the network was still able to operate because the SDN controller could still route traffic directly to R1, R2, and R5. Therefore, all the scenarios clearly showed that the SDN model can be applied to contain sniffing and DDoS attacks in MIPv6.

*Objective 2: Explore effects of Sniffing and DDoS security threats in Mobile Internet Protocol version 6 (MIPv6)*

It was validated by the study that, like in the case of the traditional wireless network models, software-defined networking wireless network models are faced with the same security challenges such as DDoS attack and sniffing attack. Both the sniffing and the DDoS attacks compromise the network in many ways. Specifically, the study found out that the two attacks led to the rerouting of traffic to unintended destinations i.e., to R4 and then to S4 instead of R1 to S2. Likewise, under the DDoS attack, networks suffered from spamming of fake packets generated by the attacker node leading to an increased number of fake packets in the network. Further, under such attacks, network components were compromised leading to the registration of incorrect network status in the affected routing tables of the affected routers.

*Objective 3: Determine Software-Defined Networking mechanisms for containing Sniffing and DDoS security threats in Mobile Internet Protocol version 6 (MIPv6)*

The study established that a software-defined networking model had inbuilt mechanisms that enabled them to contain security threats in Mobile Internet Protocol version 6 environments. The mechanisms came into play because of the programmability nature of the SDN. The architecture of the SDN showed the different inbuilt components that the model employed to achieve this effectiveness. The mechanisms included, but are not limited to the use of HashMap, having knowledge of all network components and states, disabling compromised network components, segregation between the data plane and the control plane, and load balancing among different routes in a network. Such mechanisms worked in synchronicity to contain the challenges of the sniffing and DDoS attacks and achieve efficiency in such networks.

*Objective 4: Show that the Software-Defined Networking model can better contain Sniffing and DDoS security threats in MIPv6 as compared to traditional network models*

From the findings, it was observable that the simulated topology without the SDN registered a higher number of packet flows per unit second as compared to the simulated topology with the SDN model under both sniffing and DDoS. In the case of the network without the SDN, the malicious activities of the hacker node could not be stopped as there was no other component with the knowledge that the network had been compromised. Under the DDoS attack without the SDN, the attacker node redirected huge amounts of traffic to the servers, routers, and to the other network components rendering the webserver inoperable. The reason for the low packet count in both the attacks with the SDN in place was that the controller was able to detect unusual behaviour in the network originating from the hacker node and subsequently responded by employing the containment mechanisms. The study, therefore, concluded that the Software-Defined Networking was a better model to contain both sniffing and DDoS attacks in Mobile IP version 6 as compared to the traditional models.

### **5.3 Conclusion**

The study concluded that the SDN model could indeed be applied in the MIPv6 environment to contain both DDoS attack and Sniffing attack. The findings of the study extended the conclusions of Kreutz et al. (2015), Lara (2016), Othmane et al. (2017), Rene (2018) as well as Kanniga & Murugaboopathi (2018) which affirmed that the SDN had the advantage of containing the threats posed by the two attacked in regards to mobility. In the case of the MIPv6, the findings agreed that the SDN model could effectively control the unusual behaviour of the attacker node of injecting sniffing the DDoS attacks in a network. The SDN could also provide alternative routes to the benign packets where links between any network components are compromised leading to the normal operation of the network.

The study further noted that the use of the SDN model had far-reaching benefits in controlling network insecurity as compared to the legacy or traditional models. It also concurred with the findings of Kreutz et al (2015) that, when the SDN model was used, the various components and processes of the network could be well coordinated to augment performance of a network. The study also concluded that the Software-Defined Networking had a number of functionalities that enabled it to achieve this namely, segregation of data and control planes, having overall knowledge of the network, and load balancing among others. The Software-Defined Networking model, therefore, could manage both the sniffing and DDoS attacks in MIPv6 better than in traditional network models.

#### **5.4 Recommendation for Policy and Practice**

The discussions and findings of the study which pursued the use of the Software-Defined Networking model to contain security threats in the Mobile Internet Protocol version 6, would be important for policy and practice. For example, the findings of the study would be beneficial in network design considerations to help come up with more resilient network architectures in the wake of rampant security attacks. The study would also be helpful in the formulation of policies around network security measures in not only wireless topologies but wired and hybrid topologies. In the same vein, the findings would be instrumental in augmenting the advancement of research in network security models particularly in enriching the security knowledge base for future researchers and other consumers of the knowledge such as the government and security experts.

## 5.5 Limitations of the Study

The study advanced concepts and theories that showed clearly the importance of using the Software-Defined Networking model to contain security threats in MIPv6. While applying Border Gateway Protocol and, and Open Shortest Path First in tuning the simulated topologies to behave in a particular way, there was still room to include more advanced protocols such as terminal over a network (telnet) and Address Resolution Protocol (RARP) to show more behaviours and findings from the use of the software-defined networking model to improve security in MIPv6.

The study also focused on one model (Software-Defined Networking) although there were other models such as the Root cause analysis model and the Machine Learning model that could have also been applied to determine their effectiveness in containing insecurity challenges in the MIPv6. By applying the emerging models also, future studies would compare the models and recommend a better one or grade them accordingly. This is because network security is an ever-evolving discipline that requires an amalgamation of many tools, concepts, and models to catch up with the challenges of network insecurity.

Last, but not least, there was room to use other network simulation tools such as Python as a coding language to simulate the client, server, and router classes in the virtual working environment through the application of the concept of queue data structure to store and forward the packets from one node to the other in the network. This would enable comparative analysis of findings obtained from different simulated network topologies. In this way, more thoughts and ideas would be provoked in the minds of researchers to make more discoveries and conclusions about the management of network insecurity challenges in the industry.



## **5.6 Suggestions for Further Study**

The software-defined networking model was a reliable tool that helped to address security challenges in the Mobile Internet Protocol version 6 (MIPv6) environment. Further studies could still be conducted using more protocols such as terminal over a network (telnet) and Reverse Address Resolution Protocol (RARP) to provide more findings and conclusions. Future studies could still be incorporated to include more concepts on software-defined networking, MIPv6, and network security approaches and also extend the scope of the objectives of the that were not included in the study. Last, but not least, if the research could also be conducted using other models such as the Root cause analysis model and Machine Learning model then more conclusions and findings could be deduced on containment of security challenges in MIPv6.

## REFERENCES

- Abdel, R. A., & Hatem, S. (2011). Security issues with Mobile IP Master's Thesis in Computer Network Engineering. Retrieved from <http://www.diva-portal.org/smash/get/diva2:404239/FULLTEXT01>
- Ahmad, R., Marc, S., & Christian, M. (2016). Efficient handover with optimized localized routing for Proxy Mobile IPV6, 62 (4): 75-693. Retrieved from <https://econpapers.repec.org/scripts/search.pf?ft=Mobile+IPV6>
- Andrea, F. (2018). IoT Simulations with Cisco Packet Tracer. Retrieved from <https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf?sequence=1&isAllowed=y>
- Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in Internet of Things and wearable devices. *IEEE Trans. Multi-Scale Comput. Syst.*, 1 (2): 99-109.
- Bakhshi, T. (2018). Securing Wireless Software Defined Networks: Appraising Threats, Defenses & Research Challenges. *International Conference on Advancements in Computational Sciences (ICACS)*.
- Charalampos, R., Daniel, K., Arsham, F., Jamie, B., Lyndon, F., Nektarios, G.,... David, H. (2017). Network service orchestration standardization: A technology survey. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0920548916302458>
- Corporate Social Responsibility. (2018). Retrieved from Cisco: <https://www.cisco.com/c/en/us/about/csr.html>
- Cox, J. H., Clark, R. J., & Owen, H. L. (2016). Security transition policy framework for software-defined networks. *IEEE Conference on Network Function Virtualization and Software Defined Networks (SDN-NFV) Palo Alto*, 56-61. DOI: 10.1109 / NFV-SDN.2016.7919476.
- Fatema, T. Z., Samiul, A., & Mahbubur, R. (2014). Mobile IPV6 mobility management and security aspects. *International Journal of Computational Science and Engineering*. Retrieved from [https://www.researchgate.net/publication/264974205\\_Overview\\_of\\_IPV6\\_Mobility\\_Management\\_Protocols\\_and\\_their\\_Handover\\_Performances](https://www.researchgate.net/publication/264974205_Overview_of_IPV6_Mobility_Management_Protocols_and_their_Handover_Performances)
- Hamid, F., Hyun, Y. L., & Akihiro, N. (2016). Software-Defined Networking: A survey *Computer Networks*, 79-95. Retrieved from [https://www.researchgate.net/publication/273398910\\_Software-Defined\\_Networking\\_A\\_survey](https://www.researchgate.net/publication/273398910_Software-Defined_Networking_A_survey)
- Hassan, Y., & Elaheh V. (2018). A Conceptual Framework and Architectural Considerations for Capability Enhancement in Software Defined Networks. Retrieved from <https://www.sid.ir/en/Journal/ViewPaper.aspx?ID=714858>

- Hiroshi, T., Keisuke, N., Masakazu, S., & Shoji, S. (2011). On applications of graph/network theory to problems in communication systems. Retrieved from <https://core.ac.uk/download/pdf/70370688.pdf>
- John W. C., (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 4: 40-44. Retrieved from [http://www.drbramedkarcollege.ac.in/sites/default/files/Research-Design\\_Qualitative-Quantitative-and-Mixed-Methods-Approaches.pdf](http://www.drbramedkarcollege.ac.in/sites/default/files/Research-Design_Qualitative-Quantitative-and-Mixed-Methods-Approaches.pdf)
- Kanniga, D. R., & Murugaboopathi, G. (2018). Application of Graph Theory Concepts in Computer Networks and its Suitability for the Resource Provisioning Issues in Cloud Computing. Retrieved from <https://thescipub.com/pdf/jcssp.2018.163.172.pdf>
- Koien, G. M. (2011). Reflections on trust in devices: An informal survey of human trust in an Internet-of-Things context. *Wireless Pers. Commun*, 61 (3): 495-510.
- Kreutz, F. M. V., Ramos, P. E., Verissimo, C. E., Rothenberg, S. A., & Uhlig, S. (2015). Software-defined networking: a comprehensive survey, *Proceedings of the IEEE*, 103(1): 14-76.
- Kristian, S., Daniel, M., & Makan, P. (2015). Identifying and addressing the vulnerabilities and security issues of SDN. *Ericsson Technology Review*. Retrieved from <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/identifying-and-addressing-the-vulnerabilities-and-security-issues-of-sdn>
- Lara, A., & Ramamurthy, B. (2016). OpenSec: Policy-Based Security Using Software Defined Networking. *IEEE Transactions on Network and Service Management*, 13(1): 30-42. DOI: 10.1109.
- Maham, I., Farwa, I., Fatima, M., Muhammad, R., & Fahad, A. (2019). Security Issues in Software Defined Networking (SDN): Risks, Challenges, and Potential Solutions. *International Journal of Advanced Computer Science and Applications*, 10(10).
- Manar, J., Taranpreet, S., Abdallah, S., Rasool, A., & Yiming, L. (2016). Software-Defined Networking: State of the Art and Research Challenges. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1406/1406.0124.pdf>
- Medaglia C. M. and Serbanati., A. (2010). An overview of privacy and security issues in the Internet of Things. *The Internet of Things*, 389-395.
- Open Networking Foundation. (2014). SDN Architecture Overview. Retrieved from [https://opennetworking.org/wp-content/uploads/2014/11/TR\\_SDN-ARCH-1.0-Overview-12012016.04.pdf](https://opennetworking.org/wp-content/uploads/2014/11/TR_SDN-ARCH-1.0-Overview-12012016.04.pdf)
- Othmane, B., Mouad, B. M., & Redouane, B. (2016). An Overview of SDN Architectures with Multiple Controllers. *Journal of Computer Networks and Communications*. Retrieved from <http://dx.doi.org/10.1155/2016/9396525>

- Perkins, C., Johnson, D., & Arko, J. (2011). Mobility Support in IPV6. *Internet Engineering Task Force (IETF)*. Retrieved from <http://www.rfc-editor.org/info/rfc6275>
- Rietz, R., Cwalinski, R., Hartmut, K., & Andreas, B. (2018). An SDN-Based Approach to Ward Off LAN Attacks. *Journal of Computer Networks and Communications*. Retrieved from <https://doi.org/10.1155/2018/4127487>
- Samuel, S. (2018). IPV6 Security Issues. Retrieved from [http://www.infosecwriters.com/text\\_resources/pdf/IPV6\\_SSotillo.pdf](http://www.infosecwriters.com/text_resources/pdf/IPV6_SSotillo.pdf)
- Scott, H., Natarajan, S., & Sezer, S. (2016). A survey of security in software-defined networks. *IEEE Communications Surveys and Tutorials*, 18(1): 623-654.
- Sicari, S., Rizzardi A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in the Internet of Things: The road ahead. *Computer Networks*, 76: 146-164.
- Stephen, I. A., & Bretta, K. M., (2016). Ethical Considerations and their Applications to Research: A Case of the University of Nairobi. *Journal of Educational Policy and Entrepreneurial Research*, 3 (12): 1-9. Retrieved from [https://profiles.uonbi.ac.ke/kuria\\_paul/files/429-825-2-pb.pdf](https://profiles.uonbi.ac.ke/kuria_paul/files/429-825-2-pb.pdf)
- Suman, D., & Anita, S. (2012). Application of Graph Theory in Communication Networks. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. 1(2). Retrieved from <https://www.ijaiem.org/volume1Issue2/IJAIEM-2012-10-11-017.pdf>
- Umma, S., & Roger, B. (2016). Research Methods for Business: A Skill-Building Approach.
- Vishal S., Ilsun, Y., Karl, A., Francesco, P., Mubashir, H., Rehmani., & Jaedeok, Lim. (2020). Security, Privacy, and Trust for Smart Mobile Internet of Things (M-IoT): A Survey. Retrieved from <https://deepai.org/publication/security-privacy-and-trust-for-smart-mobile-internet-of-things-m-iot-a-survey>
- Vishwajit, K. B., & Aumdevi, K. B. (2013). Mobile IPV6: Threats and Solution, 2(6). Retrieved from <https://ijaiem.org/Volume2Issue6/IJAIEM-2013-06-23-066.pdf>
- Wang, Z., Tao, D., & Lin, Z. (2016). Dynamic Virtualization Security Service Building Strategy for Software-Defined Networks. *12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Hefei, China*, 139-144. DOI: 10.1109.
- Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). A Survey on Software-Defined Networking. *IEEE Communications Surveys & Tutorials*, 1(17): 27-51. DOI: 10.1109 / COMST.2014.2330903.
- Xenofon, F., Mahesh, K., & Kimon, K. (2015). Software-Defined Networking Concepts. *Software-Defined Mobile Networks (SDMN)*, 3: 14-76. DOI: 10.1002 / 9781118900253.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things*, 4 (5): 1250-1258.

Zewairi, A., Suleiman, D., & Almajali, S. (2017). An Experimental Software-Defined Security check for Software Defined Network. *Fourth International Conference on Software Defined Systems (SDS)*, Valencia, Spain, 32-36. DOI: 10.1109.