JSSE JOURNAL OF SCIENCE & SCIENCE EDUCATION Vol. 6 No. 2 (Jul. – Dec. 2023): 344 - 352
Faculty of Science, Ubon Ratchathani University http://doi.org/10.14456/jsse.2023.30

Academic Article

Software-defined networks architecture enhances the security potential of adaptive networks

Natnaree Sophakan[1,*] and Phichit Sophakan[1]
[1]Faculty of Science, Ubon Ratchathani University, Thailand
**Email: natnaree.s@ubu.ac.th*

Received <24 April 2023>; Revised <22 July 2023>; Accepted <4 August 2023>

Abstract

The software can have autonomous configuration and secure network operations thanks to Software-Defined Networks (SDN) architecture. The present paper aims to present a software-defined networks architecture that enhances network security. Four themes are presented: The foundation of SDN is creating a network system so that programs can be written to manage network resources effectively in terms of time and security. The second issue outlines the three layers and two links that make up the architecture of a software-defined networks. The third issue explains the importance of SDN to the network. This topic outlines and addresses the availability, reliability, security, and performance issues network explicitly described in a secure network's system design. The final section guides creating an SDN that maximizes the network's security capabilities. The research findings that help network systems in terms of security and high efficiency from the infrastructure level to reducing maintenance costs on networking are extended in the final portion provided. Thus, research into software-defined networks designs is necessary to provide a safe network appropriate for dynamic networking technologies.

Keywords: Software-defined networks, Network security, Adaptive network

บทความวิชาการ

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ช่วยเพิ่มศักยภาพด้านความมั่นคงปลอดภัยของระบบเครือข่าย

ณัฏฐ์นรี โสภากันต์[1,*] และพิชิต โสภากันต์[1]

[1]คณะวิทยาศาสตร์ มหาวิทยาลัยอุบลราชานี จังหวัดอุบลราชานี ประเทศไทย

**Email: natnaree.s@ubu.ac.th*

รับบทความ: 24 เมษายน 2566 แก้ไขบทความ: 22 กรกฎาคม 2566 ยอมรับตีพิมพ์: 4 สิงหาคม 2566

บทคัดย่อ

ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Software-Defined Networks : SDN) เป็นสถาปัตยกรรมที่ทำให้ซอฟต์แวร์สามารถกำหนดการทำงานของเครือข่ายได้อย่างมั่นคงปลอดภัยโดยอัตโนมัติ วัตถุประสงค์ของบทความนี้เพื่อนำเสนอสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ที่ช่วยเพิ่มศักยภาพด้านความมั่นคงปลอดภัยของระบบเครือข่าย โดยนำเสนอ 4 ประเด็นได้แก่ ประเด็นแรกคือ SDN เป็นระบบเครือข่ายที่สามารถรองรับการเขียนโปรแกรมเพื่อบริหารจัดการทรัพยากร (Resources) ของระบบเครือข่ายอย่างมีประสิทธิภาพทั้งด้านเวลาและความมั่นคงปลอดภัย ประเด็นที่สองอธิบายถึงโครงสร้างของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ประกอบด้วยสามชั้นและสองการเชื่อมต่อ ประเด็นที่สามอธิบายถึงความสำคัญของ SDN ต่อระบบเครือข่ายโดยประเด็นนี้จะแยกให้เห็นถึง ความพร้อมใช้งาน (Availability) ความน่าเชื่อถือ (Reliability) ความมั่นคงปลอดภัย (Security) และประสิทธิภาพ (Performance) ซึ่งประเด็นดังกล่าวสรุปไว้ชัดเจนและได้กล่าวถึงการออกแบบระบบเครือข่ายที่มีความมั่นคงปลอดภัย และประเด็นสุดท้ายได้อธิบายถึงแนวทางในการพัฒนา SDN เพื่อช่วยเพิ่มศักยภาพด้านความมั่นคงปลอดภัยให้กับระบบเครือข่าย ซึ่งได้นำเสนอแนวทางในการวิจัยที่จะเป็นประโยชน์ต่อระบบเครือข่ายในด้านความมั่นคงปลอดภัยและการเพิ่มประสิทธิภาพ ดังนั้นการวิจัยในเรื่องการออกแบบระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN) จึงเป็นสิ่งสำคัญที่จะทำให้ระบบเครือข่ายมีความมั่นคงปลอดภัย สอดรับกับเทคโนโลยีของเครือข่ายแบบไดนามิก

คำสำคัญ: ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ความมั่นคงปลอดภัยในระบบเครือข่าย เครือข่ายที่ปรับตัวได้

บทนำ

สถาปัตยกรรมที่นำมาจัดการกับข้อมูลในองค์กรในยุคปัจจุบันต้องเป็นสถาปัตยกรรมปรับตัวได้แบบอัตโนมัติในระดับโครงสร้างพื้นฐาน สามารถจัดส่งข้อมูลได้อย่างครบสมบูรณ์ รวดเร็ว มั่นคงปลอดภัย โดยอาศัยเส้นทางการส่งข้อมูลคือระบบเครือข่ายขององค์กร ควรรองรับการขยายตัวขององค์กรที่ต้องเกิดขึ้น ระบบเครือข่ายขององค์กรมีความสำคัญมากต่อองค์กรและข้อมูลขององค์กร อีกทั้งส่งผลต่อประสิทธิภาพของการประสานงานระหว่างองค์กร ถ้าข้อมูลขององค์กรถูกทำให้เสียหายหรือข้อมูลที่เป็นความลับขององค์กรถูกขโมยไปนั้น ก็ส่งผลเสียหายต่อองค์กรอย่างยิ่ง ดังนั้นความมั่นคงปลอดภัยของข้อมูลในองค์กรจึงมีความสำคัญมากต่อองค์กร ซึ่งเส้นทางเดียวที่ทำให้องค์กรสูญเสียความมั่นคงปลอดภัยนั้นคือการโจมตีผ่านระบบเครือข่ายขององค์กร

ดังนั้นสถาปัตยกรรมที่ทันสมัยทำให้ทุกองค์กรที่ต้องการความมั่นคงปลอดภัยต้องวางโครงสร้างพื้นฐานของระบบเครือข่ายให้ดีตั้งแต่เริ่มวางระบบเครือข่ายและต้องเป็นระบบเครือข่ายที่ปรับตัวได้เพื่อรองรับการขยายตัวขององค์กร ประกอบกับยุคปัจจุบันสถาปัตยกรรมด้านฮาร์ดแวร์และซอฟต์แวร์มีความทันสมัยมากยิ่งขึ้นส่งผลให้มีซอฟต์แวร์สามารถกำหนดการทำงานของระบบเครือข่ายซึ่งเป็นฮาร์ดแวร์ได้ สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Software Defined Networks : SDN) เป็นสถาปัตยกรรมที่เป็นที่นิยมเนื่องจากมีคุณสมบัติที่สอดคล้องกับยุคสมัย โดยสถาปัตยกรรมนี้ได้แยกส่วนควบคุม (Control Plane) ออกจากส่วนของข้อมูล (Data Plane) โดยทั้งสองส่วนจะทำงานประสานกัน ซึ่งการแยกส่วนดังกล่าวส่งผลให้ระบบเครือข่ายสามารถเขียนโปรแกรมเพื่อกำหนดการทำงานของระบบเครือข่ายให้มีความมั่นคงปลอดภัย อีกทั้งสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ มีระบบรักษาความมั่นคงปลอดภัยในระดับโพรโทคอลโดยการเลือกใช้งาน Transport Layer Security หรือ TLS (Agborubere and Sanchez-Velazquez, 2017; Bholebawa and Dalal, 2018)

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์มีคุณสมบัติเด่นหลายประการในการกำหนดการทำงานของเครือข่ายให้มั่นคงปลอดภัย ประกอบกับมีหลายงานวิจัยได้กล่าวไว้ซึ่งสามารถสรุปได้ 2 กลุ่มใหญ่ ได้แก่กลุ่มที่ 1 เป็นงานวิจัยที่มุ่งเป้าด้านการศึกษาค้นคว้าการรักษาความปลอดภัยของระบบเครือข่ายโดยใช้คุณสมบัติเด่นของ SDN ในการป้องกันการโจมตีระบบเครือข่าย (Haleplidis *et al*., 2015; Hu *et al*., 2015; Li *et al*., 2016; Priyadarshini and Barik, 2022; Sophakan and Sathitwiriyawong, 2019; Swami, Dave and Ranga, 2020; Taha, 2023; Wang *et al*., 2016; Yan *et al*., 2016; Yungaicela-Naula *et al*., 2022) และกลุ่มที่ 2 เป็นงานวิจัยมุ่งเป้าด้านกำหนดการทำงานของระบบเครือข่ายโดยทำงานประสานกันระหว่าง SDN Controller กับ OpenFlow ซึ่งการทำงานในกลุ่มนี้เป็นการบริหารจัดการด้านเส้นทางการส่งข้อมูลและเป็นการป้องกันการโจมตีจาก DDoS (Feng, Mao and Jiang, 2016; Gong *et al*., 2015; Hu *et al*., 2015; Krishnan *et al*., 2023; Li *et al*., 2016; Nguyen and Yamada, 2016; Wang *et al*., 2016)

จากการศึกษางานวิจัยดังกล่าว ได้แสดงให้เห็นว่า SDN มีคุณสมบัติที่เหมาะสมกับการเป็นซอฟต์แวร์ที่ช่วยเพิ่มความมั่นคงปลอดภัยของระบบเครือข่ายในระดับโครงสร้างพื้นฐานในปัจจุบัน และในอนาคตควรมีการศึกษาค้นคว้าหรือพัฒนาระบบที่ทำงานร่วมกับ SDN เพื่อเพิ่มศักย์ภาพในการทำงานให้ระบบเครือข่ายทั้งด้านความมั่นคงปลอดภัย และด้านการบริหารจัดการข้อมูลเข้าออกในระบบเครือข่าย

วัตถุประสงค์ของการทบทวนวรรณกรรม

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN) เกิดจากแนวคิดที่ต้องการพัฒนาระบบเครือข่ายให้สามารถรองรับการเขียนโปรแกรมเพื่อเรียกใช้งานทรัพยากร (Resources) ของเครือข่ายได้ ด้วยหลักการที่สำคัญคือการทำให้เครือข่ายมีส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface : API) ซึ่งหัวข้อนี้จะกล่าวถึงสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ที่เป็นพื้นฐานในการทำความเข้าใจกับบทความจนเกิดเป็นแนวคิดในการพัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์

ความรู้พื้นฐานสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์

ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN) เป็นซอฟต์แวร์ที่ติดตั้งมาพร้อมกับอุปกรณ์เครือข่ายสวิตช์ (Switch) หรือเราเตอร์ (Router) ที่ผลิตตั้งแต่ปี พ.ศ. 2543 เป็นซอฟต์แวร์ที่ทำหน้าที่บริหารจัดการระบบเครือข่าย ซึ่งสวิตช์หรือเราเตอร์ที่ใช้ในระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ มีการแบ่งการทำงานออกเป็นสองส่วนได้แก่ ส่วนควบคุมทำหน้าที่คิดวิเคราะห์แพ็กเกจที่เข้าสู่เครือข่าย โดยกำหนดค่าในการใช้งานผ่านทางซอฟต์แวร์ที่ควบคุมจากศูนย์กลาง แล้วส่งต่อไปให้กับส่วนของข้อมูลทำหน้าที่ส่งต่อข้อมูลไปตามที่ส่วนควบคุมกำหนด โดยทั้งสองส่วนทำงานเป็นอิสระต่อกัน อุปกรณ์ทุกชิ้นในเครือข่ายต้องมีการทำงานประสานงานทั้งส่วนควบคุมและส่วนของข้อมูล

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ แบ่งออกเป็น 3 ส่วนและ 2 จุดเชื่อมต่อ ดังรูปที่ 1 ได้แก่

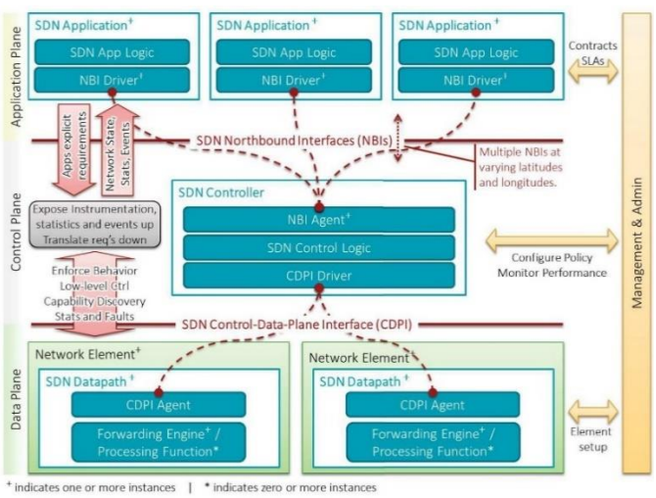
ส่วนที่ 1 ส่วนของโปรแกรม (Application Plane) ประกอบด้วย โปรแกรมประยุกต์ใช้งานบนระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN Application : SDN App) ทำหน้าที่ควบคุมการบริการจัดการเครือข่าย สามารถเขียนโปรแกรมเพิ่มเติมได้แล้วนำไปติดตั้งไว้ในส่วนนี้มี 2 ฟังก์ชันคือ SDN App Logic และ NBI Driver

ส่วนเชื่อมต่อที่ 1 อินเตอร์เฟสเชื่อมต่อส่วนบนระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN Northbound Interfaces : NBIs) เป็นอินเตอร์เฟสที่เชื่อมต่อระหว่าง SDN App กับตัวควบคุมในระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN Controller) ทำหน้าที่สร้างมุมมองของเครือข่ายในลักษณะนามธรรม (Abstract Network View) ส่งไป SDN App การที่ NBIs จะทำงานได้นั้น ส่วนของ SDN App ต้องมีฟังก์ชัน NBI Driver และ SDN Controller ต้องมีฟังก์ชัน NBI Agent

ส่วนที่ 2 ส่วนควบคุม (Control Plan) ประกอบด้วย ตัวควบคุมในระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN Controller) เป็นตัวกลางในการแปลงความต้องการจากส่วนของโปรแกรม ส่งต่อไปส่วนของข้อมูลมี 3 ฟังก์ชันได้แก่ NBI Agent, SDN Control Logic และ CDPI Driver

ส่วนเชื่อมต่อที่ 2 อินเตอร์เฟสเชื่อมต่อส่วนควบคุมและข้อมูล (SDN Control-Data-Plane Interface : CDPI) ทำหน้าที่เป็นอินเตอร์เฟสเชื่อมต่อส่วนควบคุมและส่วนของข้อมูล การที่ CDPI จะทำงานได้นั้นส่วนของ SDN Controller ต้องมีฟังก์ชัน CDPI Driver และ SDN Datapath ต้องมีฟังก์ชัน CDPI Agent แล้ว CDPI ทำงานภายใต้ความเป็นกลางไม่ขึ้นกับผู้ผลิตอุปกรณ์ ซึ่ง CDPI ที่เป็นที่นิยมและทำงานเข้ากันได้ดีในสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ได้แก่ โอเพนโฟลว์ (OpenFlow)

ส่วนที่ 3 ส่วนของข้อมูล (Data Plane) ประกอบด้วย องค์ประกอบของเครือข่าย (Network Element) หรือ เส้นทางการส่งข้อมูลของระบบเครือข่ายที่กำหนดด้วยซอฟต์แวร์ (SDN Datapath) เป็นอุปกรณ์ที่ติดตั้งในระบบเครือข่ายเพื่อควบคุมการส่งต่อข้อมูล และการประมวลผลข้อมูล มี 2 ฟังก์ชันได้แก่ CDPI Agent และ Forwarding Engine หรือ Processing Function



ภาพที่ 1 สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Software Defined Networks Architecture) (Fernandez and Munoz, 2019)

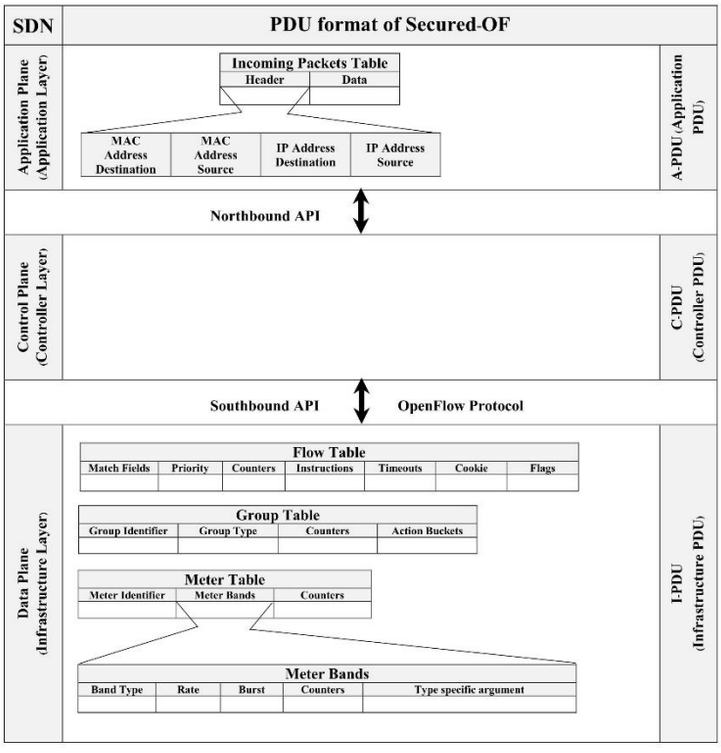
รูปแบบหน่วยข้อมูลโพรโทคอล (Protocol Data Unit : PDU) ของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ดังภาพที่ 2 ประกอบด้วย 4 เอ็นติตี้ ได้แก่

1) ตารางข้อมูลของแพ็กเกจขาเข้า (Incoming Packets Table) ประกอบด้วย Header และ Data

2) ตารางการไหล (Flow Table) ประกอบด้วย Match fields Priority Counter Instructions Timeouts Cookie และ Flags

3) ตารางกลุ่ม (Group Table) ประกอบด้วย Group identifier Group type Counters และ Action buckets

4) ตารางมิเตอร์ (Meter Table) ประกอบด้วย Meter identifier Meter bands และ Counters



ภาพที่ 2 รูปแบบหน่วยข้อมูลโพรโทคอลของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (PDU of SDN)

จากโครงสร้างการทำงานสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ มีการแยกส่วนการทำงานอย่างชัดเจน ทั้งส่วนควบคุมทำหน้าที่หลักในการควบคุมการทำงานของระบบเครือข่าย ซึ่งเป็นสมองของระบบเครือข่ายโดยอาศัยข้อมูลจากส่วนของข้อมูลที่ทำหน้าที่จดจำหรือเก็บเส้นทางการส่งข้อมูลหรือส่งแพ็กเกจ (Packet) ซึ่งแตกต่างจากระบบเครือข่ายไม่รองรับสถาปัตยกรรมระบบเครือข่ายกำหนดโดยซอฟต์แวร์ที่รวมทั้งส่วนควบคุมและส่วนของข้อมูลไว้ที่สวิตช์หรือเราเตอร์ ส่งผลให้ไม่สามารถเพิ่มศักยภาพด้านความมั่นคงปลอดภัยให้กับระบบเครือข่าย และไม่สามารถเพิ่มขนาดเครือข่ายได้อย่างอัตโนมัติซึ่งทุกองค์กรมีแนวโน้มที่จะต้องขยายตัวในอนาคต อีกทั้งยังไม่รองรับกับอุปกรณ์ทุกรุ่น หรือทุกผู้ผลิต

ความสำคัญของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ต่อระบบเครือข่าย

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์มีอิทธิพลมากต่อการออกแบบโครงพื้นฐานของระบบเครือข่ายในปัจจุบัน สาเหตุหลักเกิดจากทุกองค์กรต้องการเพิ่มประสิทธิภาพทั้งด้านความเร็วในการส่งข้อมูล ความมั่นคงปลอดภัยของระบบเครือข่ายขององค์กร และสามารถขยายเครือข่ายได้โดยอัตโนมัติโดยไม่ต้องกำหนดค่าพื้นฐานใหม่ทุกครั้งที่มีการติดตั้งอุปกรณ์เครือข่าย ซึ่งสามารถแยกความสำคัญของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ต่อระบบเครือข่าย 4 ด้าน ดังต่อไปนี้

1) ความพร้อมใช้งาน (Availability) สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ช่วยทำให้ระบบเครือข่ายพร้อมใช้งานมากยิ่งขึ้นจากคุณสมบัติดังต่อไปนี้ SDN สามารถควบคุมเครือข่ายได้โดยตรงเนื่องจาก SDN ได้มีการแบ่งส่วนการทำงานของการควบคุมออกจากส่วนของข้อมูล ผู้ดูแลระบบสามารถบริหารจัดการระบบได้ง่ายขึ้นเนื่องจากสามารถจัดการอุปกรณ์ในเครือข่าย ผ่านการกำหนดค่าโพรโทคอลโอเพนโฟลว์ และรองรับอุปกรณ์จากผู้ผลิตทุกราย SDN ใช้งานได้อย่างคล่องตัวเนื่องจากผู้ดูแลระบบสามารถบริหารจัดการการไหลของข้อมูลให้สอดคล้องกับการเปลี่ยนแปลงที่เกิดขึ้น ซึ่งมีงานวิจัยที่สอดคล้องกับความพร้อมใช้งานของระบบเครือข่ายที่ใช้ SDN ได้แก่ งานวิจัยของ Krishnan *et al*. (2023) นำเสนอ OpenStackDP ซึ่งเป็นกรอบความปลอดภัยเครือข่ายที่ปรับขนาดได้สำหรับโครงสร้างพื้นฐานคลาวด์ OpenStack ในการปรับขนาดได้ของโครงสร้างพื้นฐานคลาวด์นั้นส่งผลให้ ระบบเครือข่ายมีความพร้อมใช้งาน

2) ความน่าเชื่อถือ (Reliability) สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์มีการบริหารจัดการจากศูนย์กลาง (Centralized) ช่วยทำให้การควบคุมเครือข่ายเชิงตรรกะ (Logic) ใน SDN Controller สามารถดำเนินการได้ในครั้งเดียว อีกทั้งยังสามารถตรวจสอบการทำงานที่ผิดปกติในระบบเครือข่ายซึ่งอาจจะบ่งชี้ถึงการถูกโจมตีในเบื้องต้นและยังมีการแจ้งเตือนไปยังระบบบริหารจัดการเครือข่าย ซึ่งช่วยเพิ่มความน่าเชื่อถือให้กับระบบเครือข่าย (Krishnan *et al*., 2023;

Priyadarshini and Barik, 2022; Sophakan and Sathitwiriyawong, 2019; Swami, Dave and Ranga, 2020; Taha, 2023; Yungaicela-Naula *et al*., 2022)

3) ความมั่นคงปลอดภัย (Security) สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์สามารถกำหนดค่าบริหารจัดการระบบเครือข่าย (Configuration) ซึ่งสามารถบริหารจัดการหลัก ๆ ได้ดังนี้ การจัดการระบบเครือข่าย ความมั่นคงปลอดภัยซึ่งรวมไปถึงการปรับแต่งส่วนประกอบด้านความมั่นคงปลอดภัยและการบริหารทรัพยากรเครือข่าย ได้อย่างสะดวกรวดเร็ว ผ่าน API ที่ควบคุมจากศูนย์กลาง อีกทั้งส่วนของกำหนดค่าบริหารจัดการระบบเครือข่ายเป็นการทำงานอัตโนมัติตามที่ได้กำหนดไว้ ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์มีระบบการรักษาความมั่นคงปลอดภัยในระดับโพรโทคอลโดยการเลือกใช้งาน Transport Layer Security หรือ TLS (Agborubere and Sanchez-Velazquez, 2017; Bholebawa and Dalal, 2018) ประกอบกับ โพรโทคอลโอเพนโฟลว์ในส่วนของตัวควบคุมโอเพนโฟลว์ (OpenFlow Controller) เขียนโปรแกรมเพิ่มความมั่นคงปลอดภัยให้กับระบบเครือข่ายใช้ควบคู่กับ TLS (Meng *et al*., 2018; Tseng, Zhang and Nait-Abdesselam, 2016) ซึ่งในด้านความมั่นคงปลอดภัยของระบบเครือข่ายนั้น SDN ได้จัดการไว้เบื้องต้นในระดับดี เพื่อให้รองรับกับสถาปัตยกรรมที่ทันสมัยควรจะพัฒนาระบบรักษาความมั่นคงปลอดภัยของตัว SDN ซึ่งอาจจะเป็นช่องโหว่ในการถูกโจมตีได้ ซึ่งมีงานวิจัยที่สอดคล้องกับความมั่นคงปลอดภัยของระบบเครือข่ายที่ใช้ SDN ได้แก่ งานวิจัยของ Sophakan and Sathitwiriyawong (2019) นำเสนอสถาปัตยกรรม Secured-OF ที่มีวิธีป้องกันการโจมตีจาก DoS และ DDoS ในโพรโทคอลโอเพนโฟลว์ของ SDN ด้วยสเตทฟูลไฟร์วอลล์ ซึ่งสอดคล้องกับงานวิจัยของ Swami, Dave and Ranga (2022) นำเสนอวิธีเพิ่มความมั่นคงปลอดภัยให้ SDN ด้วยการป้องกันการโจมตีจาก DDoS อีกทั้งงานวิจัยของ Yungaicela-Naula *et al*. (2022) ได้รวบรวมประเด็นสำคัญจากงานวิจัยหลายชิ้นแล้วนำมาสรุปประเด็นสำคัญที่ส่งผลไปสู่ระบบอัตโนมัติด้านความมั่นคงปลอดภัยใน SDN

4) ประสิทธิภาพ (Performance) ระบบเครือข่ายที่มีประสิทธิภาพสูงขึ้นกับความคล่องตัวในการบริหารจัดการสามารถปรับแต่งการไหลของกระแสจราจรสำหรับเครือข่าย ตรวจสอบตำแหน่งที่ถูกโจมตีได้อย่างรวดเร็วพร้อมแจ้งเตือนและป้องกันการโจมตีได้อย่างรวดเร็ว ซึ่ง SDN ทำให้ระบบเครือข่ายมีประสิทธิภาพสูงขึ้นเนื่องจาก SDN ลดการดำเนินงานเครือข่าย (Network Operation) โดยรวมงานในระดับเลเยอร์ 2 ถึง เลเยอร์ 4 ของ OSI Model ไว้ที่การกำหนดค่าบริหารจัดการระบบเครือข่ายส่งผลให้ระบบบริหารจัดการแบบอัตโนมัติ ทำให้ประสิทธิภาพทั้งด้านเวลาและการตรวจสอบดำเนินการได้อย่างถูกต้องและรวดเร็ว อีกทั้งจำนวนสวิตช์หรือเราเตอร์ ที่มี SDN ไม่ส่งผลให้ประสิทธิภาพในทุกด้านลดลงแต่ช่วยเพิ่มประสิทธิภาพด้านการตรวจจับการโจมตีระบบเครือข่ายได้ดียิ่งขึ้นทั้งด้านเวลาและความแม่นยำในการตรวจจับ ดังนั้นเมื่อมีการขยายเครือข่ายก็สามารถดำเนินการได้อย่างง่ายโดยไม่สูญเสียประสิทธิภาพ ซึ่งประสิทธิภาพนี้ยังครอบคลุมไปถึงเรื่องงบประมาณค่าใช้จ่ายในการบำรุงรักษาระบบเครือข่าย ค่าใช้จ่ายในการขยายเครือข่าย และ SDN มีจุดเด่นที่สามารถรองรับอุปกรณ์จากผู้ผลิตหลาย ๆ ราย ซึ่งมีงานวิจัยที่สอดคล้องกับประสิทธิภาพด้านความมั่นคงปลอดภัยของระบบเครือข่ายที่ใช้ SDN ได้แก่ งานวิจัยของ Priyadarshini and Barik (2022) นำเสนอวิธีเพิ่มประสิทธิภาพด้านความมั่นคงปลอดภัยด้วยการใช้โมเดลการเรียนรู้เชิงลึก (Deep Learning Model) เพื่อเรียนรู้รูปแบบการโจมตี DoS แล้วนำรูปแบบที่ได้ส่งกลับไปให้กฎการไหล (Flow Rule) ใช้เป็นข้อมูลในการวิเคราะห์การโจมตีจาก DDoS เช่นเดียวกับงานวิจัยงานวิจัยของ Sophakan and Sathitwiriyawong (2019) นำเสนอสถาปัตยกรรม Secured-OF ที่มีวิธีการเพิ่มประสิทธิภาพด้านความมั่นคงปลอดภัยด้วยการใช้แบบจำลองเครือข่ายเบส์แบบไดนามิก (Dynamic Bayesian Network Model) เพื่อเรียนรู้รูปแบบการโจมตี DoS และ DDoS แล้วนำรูปแบบที่ได้ส่งกลับไปให้สเตทฟูลไฟร์วอลล์เพื่อเพิ่มกฎการกรองการโจมตีจาก DoS และ DDoS และยังสอดคล้องกับงานวิจัยของ Taha (2023) นำเสนอวิธีในการปรับการกำหนดเส้นทางตามตัวควบคุมเครือข่ายที่มีประสิทธิภาพเพื่อเพิ่ม QoE ของบริการสตรีมมิ่งมัลติมีเดีย

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์มีความสำคัญต่อระบบเครือข่ายทั้งที่ใช้งานในปัจจุบันและเครือข่ายที่คาดว่าจะขยายตามขนาดขององค์กรซึ่งเกิดขึ้นกับทุกองค์กร ทั้งด้านความพร้อมใช้งาน ด้านความน่าเชื่อถือ ด้านความมั่นคงปลอดภัย และ ด้านประสิทธิภาพความถูกต้องแม่นยำพร้อมทั้งใช้เวลาการประมวลผลได้อย่างรวดเร็ว คุณสมบัติเด่นของระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ที่มีความสำคัญต่อระบบเครือข่ายคือ SDN แยกส่วนควบคุมออกจากส่วนของข้อมูลทำให้ SDN ซึ่งเป็น API สามารถควบคุมการทำงานของระบบเครือข่ายได้ง่ายอย่างอัตโนมัติด้วยการกำหนดค่าบริหารจัดการระบบเครือข่าย และมีส่วนที่เป็นฐานข้อมูลที่จัดเก็บลักษณะการโจมตีที่สามารถปรับปรุงพัฒนาได้ ในส่วนนี้มีหลายงานวิจัยที่พัฒนาเสร็จสิ้นและกำลังจะพัฒนา ที่มีข้อดีและข้อเสียแตกต่างกันไป ซึ่งทั้งหมดนี้ไปช่วยลดค่าใช้จ่ายในการบำรุงรักษาระบบเครือข่าย การขยายระบบเครือข่าย ด้วยเหตุนี้ที่ทำให้ระบบเครือข่ายที่มีอุปกรณ์ที่ต่อเชื่อมในเครือข่ายที่เป็นสวิตช์หรือเราเตอร์ที่มีสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ติดมาด้วยจึงเป็นระบบเครือข่ายที่ทำงานได้ประสิทธิภาพสูงกว่าระบบเครือข่ายทั่วไป

การออกแบบระบบเครือข่ายที่มีความมั่นคงปลอดภัย

การออกแบบระบบเครือข่ายให้มีความมั่นคงปลอดภัย ควรออกแบบให้เหมาะสมกับแนวโน้มของเครือข่ายเสมือนจริง สามารถปรับเปลี่ยนได้อย่างอัตโนมัติ มีความยืดหยุ่นในการทำงาน ซึ่งมีหลักการในการออกแบบดังนี้

ออกแบบเครือข่ายโดยลดความซ้ำซ้อนของเครือข่ายหลัก

เลือกอุปกรณ์ที่มีสถาปัตยกรรมยืดหยุ่น มีประสิทธิภาพ ทำงานแบบอัตโนมัติ เพื่อลดความซ้ำซ้อนในการ กำหนดค่าบริหารจัดการระบบเครือข่าย อีกทั้งควบคุมการทำงานของระบบเครือข่าย รวมไปถึงการเพิ่มขนาดของเครือข่ายในอนาคตได้ การออกแบบเครือข่ายโดยลดความซ้ำซ้อนของเครือข่ายหลักนั้นควรถูกดำเนินการตั้งแต่เริ่มทำการติดตั้งโครงสร้างพื้นฐาน ด้วยกำหนดค่าหรือการทำคอนฟิกุเรชันบริหารจัดการเครือข่ายแบบอัตโนมัติ เมื่อระบบเครือข่ายขององค์กรถูกใช้งานไประยะเวลาหนึ่ง องค์กรมีความมั่นคงของระบบเครือข่ายองค์กร ด้วยขนาดขององค์กรที่ใหญ่ขึ้นส่งผลให้ระบบเครือข่ายองค์กรขาดความปลอดภัย เช่น เว็บไซต์องค์กรไม่สามารถให้บริการแก่ลูกค้าจำนวนมากได้เนื่องจากประสิทธิภาพของเครื่องแม่ข่ายที่เก็บข้อมูลเว็บไซต์มีไม่เพียงพอต่อการให้บริการลูกค้าและล้าสมัย เป็นต้น ดังนั้นเพื่อให้เกิดความปลอดภัยต่อเครือข่ายองค์กรต้องมีการขยายขนาดของเครือข่ายทั้งการเพิ่มเครื่องแม่ข่าย เพิ่มเครื่องลูกข่าย เพิ่มอุปกรณ์สื่อสาร เช่น สายสัญญา สวิตช์ เราเตอร์ เป็นต้น ซึ่งอุปกรณ์ทุกชิ้นที่เชื่อมต่อเข้ากับระบบเครือข่ายเดิมขององค์กร ควรจะสามารถใช้งานระบบเครือข่ายได้ทันทีแบบอัตโนมัติโดยไม่ต้องไปกำหนดค่าใหม่ การทำเช่นนี้ช่วยลดความซ้ำซ้องของเครือข่ายหลักได้ ซึ่งหลักการนี้สอดคล้องกับประโยชน์ของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Feng, Mao and Jiang, 2016; Gong *et al*., 2015)

ออกแบบเครือข่ายให้เป็นนามธรรม สามารถจัดการทรัพยากรของเครือข่ายได้ทุกชนิดทุกผู้ผลิต

ช่วยควบคุมเส้นทางของการส่งแพ็กเกจ ตรวจสอบข้อผิดพลาดของแพ็กเกจ ซึ่งสามารถตั้งข้อสังเกตในเบื้องต้นว่าระบบเครือข่ายกำลังถูกโจมตี อีกทั้งยังเป็นหนึ่งในกลยุทธ์การรักษาความมั่นคงปลอดภัยเครือข่าย การออกแบบเช่นนี้ช่วยลดความไม่สอดคล้องของการกำหนดค่าเครือข่ายหรือลดข้อผิดพลาด ควบคุมการส่งแพ็กเกจในเส้นทางที่ดีที่สุด สรุปการออกแบบเช่นนี้เป็นการเพิ่มประสิทธิภาพของเครือข่าย และเป็นการเพิ่มความมั่นคงปลอดภัยให้กับเครือข่าย การออกแบบเครือข่ายให้เป็นนามธรรม องค์กรที่มั่นคงต้องมีการขยายขนาดขององค์กรอย่างหลีกเลี่ยงไม่ได้ ด้วยเหตุผลด้านความมั่นคงปลอดภัยขององค์กรซึ่งส่งผลให้ระบบเครือข่ายองค์กรต้องขยายขนาดเช่นกัน การเพิ่มอุปกรณ์เครือข่ายทุกชนิดนั้นไม่จำเป็นจะต้องยึดติดกับผู้ผลิต ซึ่งสถาปัตยกรรมเครือข่ายแบบเดิมทุกครั้งที่มีการเพิ่มอุปกรณ์เครือข่ายใด ๆ หรืออุปกรณ์เครือข่ายที่ต่างผู้ผลิตก็ต้องมากำหนดค่าของระบบเครือข่ายใหม่ทุกครั้งซึ่งทำให้องค์กรต้องเสียงบประมาณ เสียเวลาในการกำหนดค่าตามผู้ผลิตกำหนด ซึ่งทำให้เกิดความยุ่งยากซับซ้อนทุกครั้งที่ต้องขยายขนาดของระบบเครือข่ายที่ต้องเกิดขึ้นกับทุกองค์กรโดยหลีกเลี่ยงไม่ได้ ดังนั้นการออกระบบเครือข่ายควรออกแบบเครือข่ายให้เป็นนามธรรม สามารถจัดการทรัพยากรของระบบเครือข่ายได้ทุกชนิดทุกผู้ผลิต ซึ่งสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Feng, Mao and Jiang, 2016; Gong *et al*., 2015) สามารถทำได้ ไม่ว่าจะติดตั้งอุปกรณ์เครือข่ายชนิดใด ผู้ผลิตรายใด เข้ามาในระบบเครือข่าย อุปกรณ์เครือข่ายนั้น ก็สามารถใช้งานในระบบเครือข่ายได้ทันที

ออกแบบโครงสร้างพื้นฐานของเครือข่ายโดยไม่ยึดติดกับผู้ผลิต

ควรเลือกทรัพยากรที่ใช้ในระบบเครือข่ายที่ดีที่สุดเหมาะสมกับโครงสร้างพื้นฐานของเครือข่ายที่ออกแบบมากที่สุดและทรัพยากรนั้นควรเป็นอิสระจากผู้ผลิต สามารถใช้งานร่วมกันได้หลากหลายผู้ผลิต ซึ่งการออกแบบเช่นนี้เป็นการ ปลดล็อกหรือมองข้ามข้อจำกัดเรื่องทรัพยากร ส่งผลให้การออกแบบโครงสร้างพื้นฐานของเครือข่ายดำเนินการได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัยยิ่งขึ้น

จากหลักการทั้ง 3 ประเด็นนั้นสอดคล้องกับประโยชน์ของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Feng, Mao and Jiang, 2016; Gong *et al*., 2015) ซึ่งสามารถสรุปในเบื้องต้นได้ว่า สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ เหมาะสมกับการนำมาใช้ในการออกแบบโครงสร้างพื้นฐานของระบบเครือข่ายและปรับปรุงระบบเครือข่าย

แนวทางในการพัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ที่ช่วยเพิ่มความมั่นคงปลอดภัยให้กับระบบเครือข่าย

ในช่วงปีที่ผ่านมา ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ได้รับการยกฐานะเป็นสถาปัตยกรรมที่นิยมมากในการนำมาใช้ในระบบเครือข่ายและมีนักวิจัยสนใจพัฒนาสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์มากขึ้น เพื่อเป็นแนวทางในการพัฒนาและเป็นกรอบกว้าง ๆ ให้กับนักวิจัย ซึ่ง Yan *et al*. (2016) ได้สรุปแนวทางในการพัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ที่น่าสนใจไว้ 3 แนวทางดังนี้

1. พัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ เพื่อบริหารจัดการข้อมูลขนาดใหญ่ (SDN developed to manage the Big Data)

ได้กล่าวถึงการโจมตีจาก DDoS ซึ่ง ในปัจจุบันมีการปรับปรุงรูปแบบให้มีการโจมตีแบบเพิ่มขนาดอย่างรวดเร็วซึ่งเป็นการโจมตีแบบรุนแรงและรวดเร็ว โดยอาศัยสถาปัตยกรรมอินเตอร์เน็ตความเร็วสูง มีการใช้ประโยชน์จากบอตเน็ต (Botnets) ลักษณะการเพิ่มการโจมตีที่มีการเพิ่มขนาดอย่างรวดเร็ว ขนาดของข้อมูลเหล่านั้นจะมีความซับซ้อนและมีขนาดใหญ่ (Big Data) ซึ่งการตรวจจับการโจมตี เมื่อมีการพัฒนาระบบเครือข่ายให้รองรับการรับส่งข้อมูลหรือแพ็กเกจขนาดใหญ่ที่มีความซับซ้อนได้จะเป็นการแก้ปัญหาการโจมตีระบบเครือข่าย

การพัฒนาเครือข่ายให้รองรับกับข้อมูลขนาดใหญ่ที่มีความซับซ้อน สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ มีความเหมาะสมมากที่สุดในการนำมาพัฒนาเพื่อบริหารจัดการข้อมูลขนาดใหญ่ที่มีความซับซ้อน เนื่องจาก SDN สามารถตั้งค่าการบริหารจัดการเครือข่ายให้ทำงานแบบอัตโนมัติได้ จึงส่งผลถึงการขยายเครือข่ายได้โด ยอัตโนมัติโดยไม่ต้องปรับเปลี่ยนค่าใด ๆ

2. พัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ เพื่อบริหารจัดการฟังก์ชันเครือข่ายเสมือนจริง (SDN developed to manage the Network Function Virtualization : NFV)

ฟังก์ชันเครือข่ายเสมือนจริงมีการนำมาใช้ในเครือข่ายเสมือนจริง (Network Virtualization : NV) และเครือข่ายเสมือนจริงหลายเครือข่าย (Multiple Virtual Network : VNs) ส่งผลดีให้สามารถใช้ทรัพยากรเครือข่ายร่วมกันได้ตั้งแต่ระดับโครงสร้างพื้นฐาน นอกจากนี้เครือข่ายเสมือนจริงช่วยให้ควบคุมการไหลของแพ็กเกจ และเป็นการควบคุมแบบรวมศูนย์

SDN เป็นสถาปัตยกรรมที่เหมาะสำหรับการนำมาพัฒนาเพื่อบริหารจัดการฟังก์ชันเครือข่ายเสมือนจริงเพราะ SDN มีการติดตั้งมากับสวิตช์หรือเราเตอร์ มีตรรกะควบคุมการทำงานทรัพยากรเครือข่ายและสามารถกำหนดค่าบริหารจัดการ ระบบเครือข่าย

3. พัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์เพื่อเป็นศูนย์กลางข้อมูลเครือข่าย (SDN developed to Information-Centric Networking)

ศูนย์กลางข้อมูลเครือข่าย (Information-Centric Network : ICN) เป็นสถาปัตยกรรมใหม่ที่ได้รับการเสนอเป็นวิธีแก้ปัญหาสำหรับการเพิ่มประสิทธิภาพของการจัดส่งแพ็กเกจและความพร้อมของแพ็กเกจ เป็นสถาปัตยกรรมเครือข่ายที่มีอิสระในเรื่องสถานที่ มีการแยกส่วนระหว่างส่วนควบคุมแพ็กเกจและส่วนของการส่งต่อแพ็กเกจซึ่งสอดคล้องกับหลักการของ SDN โดยมีโพรโทคอลโอเพนโฟลว์ (OpenFlow Protocol) เป็นตัวกลางสำหรับการย้ายแพ็กเกจ ดังนั้นในกลุ่มงานวิจัยพัฒนาระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์เพื่อเป็นศูนย์กลางข้อมูลเครือข่าย ควรมุ่งศึกษา OpenFlow-based

สรุปผลและข้อเสนอแนะ

สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ เป็นสถาปัตยกรรมรูปแบบใหม่ที่ทำให้ซอฟต์แวร์กำหนดค่าบริหารจัดการระบบเครือข่ายได้ตั้งแต่ระดับโครงสร้างพื้นฐาน อีกทั้งยังสามารถขยายระบบเครือข่ายได้โดยอัตโนมัติ ไม่ต้องกำหนดค่าใหม่เมื่อมีการติดตั้งอุปกรณ์เครือข่ายเพิ่มเติม ประกอบกับคุณสมบัติเด่นของระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์สามประการได้แก่ ประการที่ 1 สถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ สามารถทำให้เครือข่ายมี API ซึ่งหมายถึงระบบเครือข่ายสามารถรองรับการเขียนโปรแกรมเพื่อเรียกใช้งานทรัพยากร (Resources) ของระบบเครือข่ายได้ แบ่งการทำงานออกเป็นสองส่วนได้แก่ ส่วนควบคุมและส่วนของข้อมูล ประการที่ 2 ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ สามารถกำหนดค่าบริหารจัดการระบบเครือข่ายอัตโนมัติ ซึ่งสามารถบริหารจัดการระบบเครือข่าย ความมั่นคงปลอดภัยซึ่งรวมไปถึงการปรับแต่งส่วนประกอบด้านความมั่นคงปลอดภัยและการบริหารทรัพยากรระบบเครือข่าย ได้อย่างสะดวกรวดเร็ว ผ่าน API ที่ควบคุมจากศูนย์กลาง และประการสุดท้าย มีส่วนของฐานข้อมูลที่เก็บลักษณะการโจมตี เส้นทางการโจมตีของอุปกรณ์ระบบเครือข่ายที่ถูกโจมตี ไว้ที่โอเพนโฟลว์ (OpenFlow)

จากคุณสมบัติเด่นสามประการของสถาปัตยกรรมระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ ส่งผลให้ระบบเครือข่ายมั่นคงปลอดภัยและประสิทธิภาพสูงตั้งแต่ระดับโครงสร้างพื้นฐาน ประหยัดค่าใช้จ่ายในการบำรุงรักษาเครือข่าย และเป็นอีกหนึ่งสถาปัตยกรรมที่ควรนำมาวิจัยพัฒนาเพื่อให้ระบบเครือข่ายมีความมั่นคงปลอดภัยสอดรับกับสถาปัตยกรรมแบบไดนามิก

References

Agborubere, B. and Sanchez-Velazquez, E. (2017). OpenFlow communications and TLS security in software-defined networks. **Proceedings of 2017 IEEE International Conference on Internet of Things (iThings)**

and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), (pp. 560–566). Exeter: IEEE.

Bholebawa, I. Z. and Dalal, U. D. (2018). Performance analysis of SDN/OpenFlow controllers: POX versus floodlight. **Wireless Personal Communications**, 98(2), 1679–1699.

Feng, M., Mao, S. and Jiang, T. (2016). Enhancing the performance of future wireless networks with software-defined networking. **Frontiers of Information Technology & Electronic Engineering**, 17(7), 606–619.

Fernandez, C. and Munoz, J. L. (2019). Software Defined Networking (SDN) with OpenFlow 1.3 Open vSwitch and Ryu. Retrieved 7 May 2023, from **UPC Telematics Department:** https: / / upcommons. upc.edu/bitstream/handle/2117/77684/sdn-book.pdf.zip

Gong, Y., Huang, W., Wang, W. and Lei, Y. (2015). A survey on software defined networking and its applications. **Frontiers of Computer Science**, 9(6), 827–845.

Haleplidis, E., Hadi Salim, J., Denazis, S. and Koufopavlou, O. (2015). Towards a network abstraction model for SDN. **Journal of Network and Systems Management,** 23(2), 309–327.

Hu, Y., Wang, W., Gong, X., Que, X. and Cheng, S. (2015). On the feasibility and efficacy of control traffic protection in software defined networks. **Science China Information Sciences**, 58(12), 1–19.

Krishnan, P., Jain, K., Aldweesh, A., Prabu, P. and Buyya, R. (2023). OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. **Journal of Cloud Computing**, 12(26), 1-42.

Li, D., Wang, S., Zhu, K. and Xia, S. (2017). A survey of network update in SDN. **Frontiers of Computer Science**, 11(1), 4–12.

Meng, W., Choo, K.-K. R., Furnell, S., Vasilakos, A. V. and Probst, C. W. (2018). Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks. **IEEE Transactions on Network and Service Management**, 15(2), 761–773.

Nguyen, K. and Yamada, S. (2016). An experimental feasibility study on applying SDN technology to disaster-resilient wide area networks. **Annals of Telecommunications**, 71(11), 639–647.

Priyadarshini, R. and Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. **Journal of King Saud University - Computer and Information Sciences**, 34(3), 825–831.

Sophakan, N. and Sathitwiriyawong, C. (2019). A Secured OpenFlow-Based Software Defined Networking Using Dynamic Bayesian Network. **Proceedings of 2019 19th International Conference on Control, Automation and Systems (ICCAS),** (pp. 1517–1522). Exeter: IEEE.

Swami, R., Dave, M. and Ranga, V. (2020). Software-defined Networking-based DDoS Defense Mechanisms. **ACM Computing Surveys**, 52, 1–36.

Taha, M. (2023). An efficient software defined network controller based routing adaptation for enhancing QoE of multimedia streaming service. **Multimedia Tools and Applications**, 94(2), 1-24.

Tseng, Y., Zhang, Z. and Nait-Abdesselam, F. (2016). ControllerSEPA: A security-enhancing SDN controller plug-in for OpenFlow applications. **Proceedings of 2016 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT),** (pp. 268–273). Exeter: IEEE.

Wang, Y., Bi, J., Lin, P., Lin, Y. and Zhang, K. (2016). SDI: a multi-domain SDN mechanism for fine-grained inter-domain routing. **Annals of Telecommunications**, 71(11), 625–637.

Yan, Q., Yu, F. R., Gong, Q. and Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. **IEEE Communications Surveys & Tutorials**, 18(1), 602–622.

Yungaicela-Naula, N. M., Vargas-Rosales, C., Perez-Díaz, J. A. and Zareei, M. (2022). Towards security automation in Software Defined Networks. **Computer Communications**, 183, 64-82.