วารสารวิชาการ กสทช.
ประจำปี 2563

NBTC JOURNAL 2020

สำนักงานคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
Office of the National Broadcasting and Telecommunications Commission

ความมั่นคงปลอดภัยไซเบอร์ สำหรับโครงข่าย 5G

CYBERSECURITY FOR 5G NETWORK

สุรชัย ฉัตรเฉลิมพันธุ์ [1] และ เทอดพงษ์ แดงสี [2]

Surachai Chatchalermpun [1] and Therdpong Daengsi [2]

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเอเชียอาคเนย์ กรุงเทพฯ 10160 [1]
สาขาวิศวกรรมการจัดการอุตสาหกรรมเพื่อความยั่งยืน คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร กรุงเทพฯ 10300 [2]
Computer Engineering, Faculty of Engineering, Southeast Asia University,
Bangkok 10160 Thailand [1]
Sustainable Industrial Management Engineer, Faculty of Engineering,
Rajamangala University of Technology Phra Nakhon, Bangkok 10330 Thailand [2]

Corresponding E-mail : Therdpong.d@rmutp.ac.th

Received Date June 15, 2020
Revised Date July 8, 2020
Accepted Date October 29, 2020

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในการนำเสนอเรื่องความมั่นคงปลอดภัยไซเบอร์สำหรับ โครงข่าย 5G ที่เริ่มเปิดใช้งานในประเทศไทยในช่วงปลายไตรมาสที่ 1/2563 โดยศึกษาทบทวนวรรณกรรมและรวบรวมข้อมูลที่เกี่ยวข้องกับบทบาทหน้าที่และบริบทของโครงข่าย 5G ซึ่งประกอบด้วยเครือข่ายต้นน้ำ กลางน้ำ และปลายน้ำ นอกจากนี้ยังได้ศึกษาข้อเสนอแนะด้านความมั่นคงปลอดภัยไซเบอร์จากองค์กรต่าง ๆ ที่เกี่ยวข้อง ผลการศึกษาพบว่า เครือข่ายต้นน้ำ กลางน้ำ และปลายน้ำ ต่างมีความเสี่ยงต่อการถูกคุกคาม เช่น การโจมตีให้เกิดการปฏิเสธการให้บริการ การเกิดความคับคั่งของการจราจรข้อมูล และการโจมตีแบบแทรกกลางการสื่อสาร ฯลฯ จึงเป็นเรื่องท้าทายและจำเป็นในการหาแนวทางป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น วิศวกรผู้ดูแลโครงข่าย 5G ต้องมีความรู้ความสามารถด้านโทรคมนาคมและการสื่อสารเป็นอย่างดี ทั้งเรื่องสมรรถนะ ประสิทธิภาพ และการประยุกต์ใช้งาน 5G รวมถึงต้องให้ความสำคัญกับการดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นข้อเสนอแนะที่สถาบันการศึกษาต่าง ๆ ควรนำไปพิจารณา

คำสำคัญ : ความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามไซเบอร์ การโจมตีทางไซเบอร์ โครงข่าย 5G

Abstract

This article aims to present the cybersecurity topic for the 5G network that has been launched in Thailand around the end of Q1/2020. The study includes literature review, and conclusive related information associated with the roles and the context of 5G networks, which consists of the upstream, middle-stream, and downstream systems. Furthermore, the study about cybersecurity recommendations from the related organizations have also conducted. From this study, it has been found that every network has some certain risks, such as Denial-of-Service (DoS) attack, traffic burst attack, and Man-in-the-Middle attack. Apparently, these are challenges and necessities to find the prevention and the solutions. Therefore, it can be concluded that cybersecurity for the 5G network becomes crucial, which is not less important than the other issues such as 5G use cases. Also, this is the reason that 5G network engineers require not only good telecommunications knowledge but also good cybersecurity knowledge. This can be academic suggestions for educational institutions to consider.

Keywords : Cybersecurity, Cyberthreats, Cyber-attacks, 5G network

บทนำ

ความมั่นคงปลอดภัยไซเบอร์

Cyber มีที่มาจากคำว่า Cybernetics ซึ่งมีความหมายเกี่ยวกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น เครือข่ายอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม ตลอดจนการให้บริการของดาวเทียม ฯลฯ (สพร., 2559) เมื่อนำมารวมกับคำว่า ความมั่นคงปลอดภัย (Security) จึงกลายเป็นคำว่า ความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้สหภาพโทรคมนาคมระหว่างประเทศ (The International Telecommunication Union : ITU) ได้ให้นิยามของคำว่าความมั่นคงปลอดภัยไซเบอร์เอาไว้ว่า เป็นชุดของเครื่องมือ นโยบาย แนวคิดการรักษาความปลอดภัย การรักษาความปลอดภัย แนวทาง วิธีการบริหารความเสี่ยง การปฏิบัติ การอบรม วิธีปฏิบัติที่เป็นเลิศ การรับประกัน และเทคโนโลยี ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ซึ่งครอบคลุมถึงอุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอปพลิเคชันบริการ ระบบสารสนเทศ และการจัดเก็บข้อมูลในไซเบอร์ (ITU-T, 2008) ฉะนั้น การรักษาความมั่นคงปลอดภัยไซเบอร์จึงอาจมีความหมายครอบคลุมถึงมาตรการ หรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกองค์กร ตลอดจนภายในและภายนอกประเทศ ซึ่งอาจมีผลกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ (ราชกิจจานุเบกษา, 2562)

ความสำคัญของ 5G

ระบบโทรศัพท์เคลื่อนที่ยุคที่ 5 (The Fifth Generation of Mobile Communications Technology : 5G) เป็นเทคโนโลยีโครงข่ายสื่อสารไร้สายความเร็วสูงที่มีแนวคิดในการออกแบบสถาปัตยกรรมโครงข่ายที่มีคุณสมบัติที่โดดเด่น ไม่ว่าจะเป็นอัตราการรับส่งข้อมูลที่สูงขึ้นประมาณ 20 เท่า เมื่อเทียบกับ 4G และค่าประวิงเวลาที่ต่ำเพียง 1 มิลลิวินาทีเท่านั้น อัตราการพร้อมใช้งาน 99.99% ความครอบคลุมพื้นที่บริการ 100% และอัตราลดการใช้พลังงานได้ 90% (Fang et al., 2018, p. 4850; เทอดพงษ์ แดงสี และพิสิฐ พรพงศ์เตชวาณิช, 2562, น. 172)

มีการประมาณการว่า หากประเทศไทยสามารถเปิดใช้งานโครงข่าย 5G ได้ภายในปี 2563 เศรษฐกิจของไทยจะเติบโตเพิ่มขึ้นเป็นอย่างมาก ดังนั้น สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) จึงได้ผลักดันให้มีการประมูลคลื่นความถี่สำหรับโครงข่าย 5G ไปเมื่อช่วงกลางไตรมาสที่ 1/2563 และปัจจุบันได้มีผู้ให้บริการโทรศัพท์เคลื่อนที่บางรายเริ่มให้บริการโครงข่าย 5G แล้ว (กสทช., 2563; ผู้จัดการออนไลน์, 2563; Techsauce, 2563)

โครงข่าย 5G ถูกออกแบบและพัฒนาให้รองรับความต้องการและการใช้งานของผู้ใช้งานที่เพิ่มมากขึ้นได้ ไม่ว่าจะเป็นการใช้งานอินเทอร์เน็ตที่เปราะบางต่อภัยทางไซเบอร์เพื่อเข้าถึงข้อมูล และการใช้งานผ่านแอปพลิเคชันและซอฟต์แวร์ต่าง ๆ ตลอดจนการบริการหรือการใช้งานหลากหลาย เช่น อาคารอัจฉริยะ (Smart building) ชุมชนอัจฉริยะ (Smart communities) เมืองอัจฉริยะ (Smart cities) โครงข่ายการดูแลสุขภาพ (Healthcare networks) โครงข่ายสื่อสารความเร็วสูง (High speed mobile networks) โครงข่ายยานพาหนะ (Vehicular networks) การสื่อสารในงานอุตสาหกรรม (Industry M2M communications) และการประมวลผลแบบกลุ่มเมฆเคลื่อนที่ (Mobile cloud computing) ฯลฯ ดังนั้น สถาปัตยกรรมและแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่เดิมใช้งานกับโครงข่าย 4G จึงไม่เหมาะสมและปลอดภัยเพียงพอสำหรับโครงข่าย 5G (Bendale & Prasad, 2018, p. 146; Ahmad et al., 2019, p. 3682; Fang et al., 2018, p. 4851; วิชัย โชควิวัฒน, 2562, น. 355)

การศึกษาบทบาทหน้าที่และบริบทของโครงข่าย 5G

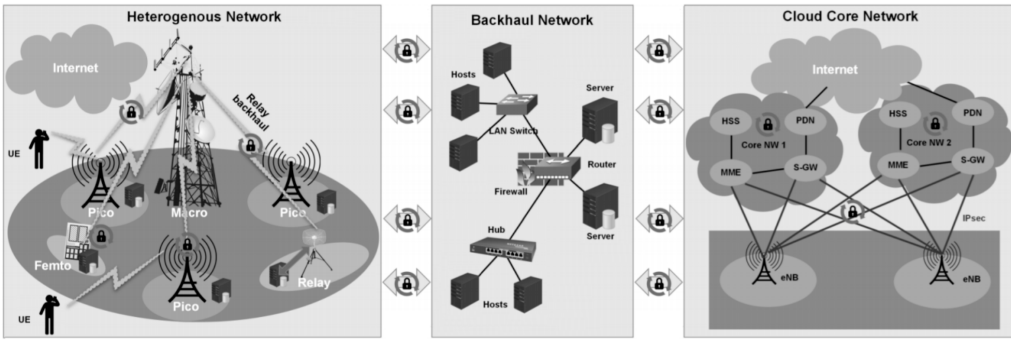
ภายในโครงข่าย 5G สามารถแบ่งออกตามบทบาทหน้าที่และบริบทของเครือข่าย ทั้งเครือข่ายต้นน้ำ เครือข่ายกลางน้ำ และเครือข่ายปลายน้ำ ที่ประกอบกันเป็นโครงข่าย 5G ซึ่งต่างมีความเสี่ยงต่อการถูกคุกคาม จึงกลายเป็นประเด็นที่ท้าทายและจำเป็นต้องหาแนวทางในการแก้ไขหากเกิดปัญหา โดยสามารถอธิบายแยกตามเครือข่ายได้เป็น 3 เครือข่าย ดังภาพที่ 1 ประกอบด้วย เครือข่ายหลักแบบกลุ่มเมฆ (Cloud core network) เครือข่ายสนธิ (Backhaul network) และ เครือข่ายระคน (Heterogeneous network: HetNet)

โดยต่อไปนี้จะเรียกว่า เครือข่ายต้นน้ำ เครือข่ายกลางน้ำ และเครือข่ายปลายน้ำ 5G ตามลำดับ เพื่อให้สอดคล้องกับบทบาทหน้าที่ของแต่ละเครือข่ายและบริบทของโครงข่าย 5G ซึ่งอธิบายได้ ดังนี้

เครือข่ายหลักแบบกลุ่มเมฆ: เครือข่ายต้นน้ำ 5G

เครือข่ายต้นน้ำ 5G หรือเครือข่ายหลักแบบกลุ่มเมฆ (Cloud core network) เป็นเครือข่ายแกนกลางของโครงข่าย 5G จึงมีอีกชื่อเรียกว่า 5G core network (5GC) ทำหน้าที่ในการจัดการการเคลื่อนที่และการเข้าถึงเครือข่าย (Access and mobility management function) การจัดการช่วงเวลาการสื่อสารหรือเซสชัน (Session management function) และการจัดการข้อมูลให้อยู่ในรูปแบบเดียวกัน (Unified data management) (Huawei, 2017)

ศักยภาพที่เพิ่มสูงขึ้นของเครือข่ายต้นน้ำ 5G เกิดจากเทคโนโลยีต่าง ๆ เช่น การจำลองเสมือนฟังก์ชันเครือข่าย (Network Function Virtualization: NFV) ซึ่งทำงานบนพื้นฐานของระบบเครื่องเสมือน หรือเวอร์ชวลแมชชีน (Virtual machine) โดยใช้เครื่องแม่ข่ายรองรับการทำงานของซอฟต์แวร์ จากเดิมที่เคยอาศัยฮาร์ดแวร์เป็นพื้นฐานบริการที่ใช้ซอฟต์แวร์เป็นพื้นฐานเหล่านี้เรียกว่า ฟังก์ชันเครือข่ายเสมือน (Virtual Network Functions: VNF) และเครือข่ายที่กำหนดโดยซอฟต์แวร์ (Software Defined Network: SDN) ซึ่งเป็นเทคโนโลยีที่เกี่ยวข้องกับการจัดการอุปกรณ์เครือข่ายรูปแบบใหม่ที่แยกส่วนการควบคุมเครือข่ายออกจากส่วนที่ทำหน้าที่บริการรับส่งข้อมูลบนเครือข่าย โดยเครือข่ายที่กำหนดโดยซอฟต์แวร์อนุญาตให้ผู้ดูแลระบบสามารถกำหนดหน้าที่การทำงานให้กับอุปกรณ์โครงข่ายได้อย่างหลากหลาย คล้ายกับกรณีที่แอปพลิเคชันบนโทรศัพท์เคลื่อนที่สามารถทำให้โทรศัพท์กลายเป็นกล้องถ่ายรูปและบัตรกดเงินสดได้ด้วย นอกจากนี้ยังรองรับการบริหารจัดการจากส่วนกลาง ณ จุดเดียวได้อย่างมีประสิทธิภาพและมีความยืดหยุ่นสูง เอื้อต่อการขยายโครงข่าย (Ahmad et al., 2019, pp. 3696-3697; วิเชียร ปรีดาลัมพะบุตร, 2563, น. 222-223; เทอดพงษ์ แดงสี และพิสิฐ พรพงศ์เตชวาณิช, 2562, น. 167-168)



ภาพที่ 1 ภาพรวมโครงข่าย 5G

Note. From “Security for 5G and Beyond” by Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M., 2019. IEEE Communications Surveys & Tutorials, 21(4), p. 3694

เครือข่ายสนธิ : เครือข่ายกลางน้ำ 5G

จากภาพที่ 1 จะเห็นได้ว่า เครือข่ายกลางน้ำ 5G หรือเครือข่ายสนธิ (Backhaul network) คือเครือข่ายส่วนที่ทำหน้าที่เป็นตัวกลางที่เชื่อมต่อเครือข่ายต้นน้ำ 5G กับเครือข่ายปลายน้ำ 5G (Ahmad et al., 2019, p. 3695) ซึ่งเครือข่ายนี้จะต้องรองรับการจราจรข้อมูล หรือทราฟฟิก (Traffic) ที่มีปริมาณมหาศาล นอกจากนี้ยังต้องมีประสิทธิภาพในการรับส่งข้อมูลสูงเพื่อรองรับสมรรถนะที่สำคัญของโครงข่าย 5G ในประเด็นที่ค่าประวิงเวลาภายในเครือข่ายจะต้องน้อยกว่า 1 มิลลิวินาที กล่าวคือ เครือข่ายกลางน้ำ 5G จะต้องทำหน้าที่ควบคุมคุณภาพของการบริการ การจัดลำดับความสำคัญในการรับส่งข้อมูล ตลอดจนการประสานเวลา (Synchronization) กับสถานีฐานย่อย (Cell site) แบบต่าง ๆ ที่อยู่ในเครือข่ายปลายน้ำ 5G อย่างไรก็ดี แม้ว่าจะมีหลายเทคโนโลยีที่อาจทำหน้าที่เป็นเครือข่ายกลางน้ำ 5G ได้ เช่น เทคโนโลยีการสื่อสารผ่านดาวเทียม แต่ด้วยข้อกำหนดและสมรรถนะของโครงข่าย 5G และความเหมาะสมหลาย ๆ ด้าน จึงทำให้เทคโนโลยีใยแก้วนำแสง (Fiber-optic) ซึ่งสามารถรองรับแบนด์วิดท์ (Bandwidth) ได้สูงสุดถึง 1,600 กิกะบิตต่อวินาทีสำหรับท่อใยแก้วนำแสงหนึ่งเส้นและมีเสถียรภาพสูง ถูกเลือกใช้ให้เป็นเทคโนโลยีหลักในการพัฒนาเครือข่ายกลางน้ำสำหรับโครงข่าย 5G ในขณะที่เทคโนโลยีไมโครเวฟซึ่งแบนด์วิดท์ได้สูงสุด 25 กิกะบิตต่อวินาทีก็ยังถือเป็นอีกทางเลือกที่ดีแม้ว่าจะมีข้อจำกัดด้านเสถียรภาพบ้างก็ตาม (Ahmad et al., 2019, p. 3695; GSMA, 2019)

เครือข่ายระคน : เครือข่ายปลายน้ำ 5G

เครือข่ายปลายน้ำ 5G หรือเครือข่ายระคน (Heterogeneous Network : HetNet) คือ เครือข่ายที่เกิดจากการผสมผสานกันระหว่างเครือข่ายที่แตกต่างกัน หรือเป็นเครือข่ายแบบหลายชั้น หรือมัลติเทียร์ (Multi-tier network) ที่ผสมผสานเทคโนโลยีไร้สายแบบต่าง ๆ ที่มีสถานีฐานติดตั้งอยู่ในบริเวณใกล้เคียงกันให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ ด้วยระบบการบริหารจัดการแบบองค์รวม เครือข่ายปลายน้ำ 5G จะรองรับสถานีฐานหลายขนาด ทั้งระดับมาโครเซลล์ (Micro cell) เฟมโตเซลล์ (Femto cell) ไปจนถึงพิโคเซลล์ (Pico cell) นอกจากนี้ ยังรวมถึงเทคโนโลยีเครือข่ายแบบไร้สาย (WiFi) ด้วย เครือข่ายปลายน้ำ 5G แก้ปัญหาคลื่นความถี่ที่มีจำกัดโดยใช้เทคนิคการใช้ความถี่ซ้ำ (Frequency reuse) เพื่อให้รองรับจำนวนผู้ใช้จำนวนมากและครอบคลุมพื้นที่ให้บริการได้กว้าง ตอบสนองความต้องการใช้งานเครือข่ายที่เพิ่มสูงขึ้นของผู้ใช้งาน ทั้งด้านคุณภาพของบริการ (Quality of service) และคุณภาพของประสบการณ์ (Quality of experience) (Ahmad et al., 2019, pp. 3692-3693; เทอดพงษ์ แดงสี และ พิสิฐ พรพงศ์เตชวาณิช, 2562, น. 169-170)

ข้อแนะนำด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงข่าย 5G

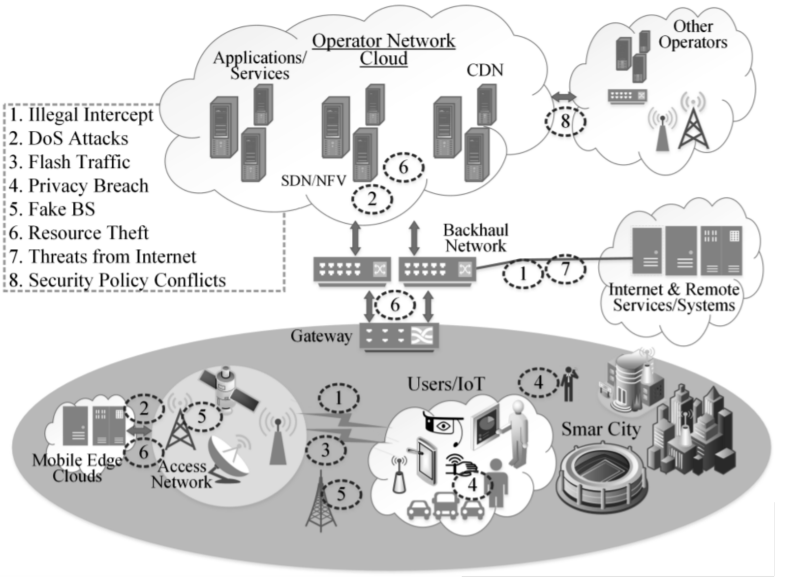
ข้อแนะนำจากสหภาพโทรคมนาคมระหว่างประเทศ

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ซึ่งเป็นองค์กรหลักในการผลักดันเทคโนโลยี 5G แบ่งความมั่นคงปลอดภัยไซเบอร์ออกเป็น 8 ด้าน ได้แก่ การควบคุมการเข้าถึง (Access control) การยืนยันตัวตน (Authentication) ไม่ปฏิเสธความรับผิด (Non-repudiation) การรักษาความลับของข้อมูล (Data confidentiality) ความปลอดภัยในการสื่อสาร (Communication security) ความสมบูรณ์ของข้อมูล (Data integrity) ความพร้อมใช้งาน (Availability) และความเป็นส่วนตัว (Privacy) ซึ่งจะเห็นได้ว่าไม่ได้ครอบคลุมเฉพาะเครือข่ายเท่านั้น แต่ครอบคลุมไปถึงแอปพลิเคชันและข้อมูลของผู้ใช้งานด้วย (Ahmad et al., 2019, p. 3691)

อย่างไรก็ดี เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว สหภาพโทรคมนาคมระหว่างประเทศได้กำหนดเป็นข้อแนะนำขึ้นโดยครอบคลุมการรักษาความมั่นคงปลอดภัยทั้งในโครงข่ายการสื่อสารโทรคมนาคมและอินเทอร์เน็ต ไม่ว่าจะเป็นโครงข่ายโทรคมนาคมยุคหน้า (Next Generation Network : NGN) อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things: IoT) และการประมวลผลกลุ่มเมฆหรือ Cloud computing นอกจากนี้ สหภาพโทรคมนาคมระหว่างประเทศ ยังมีข้อแนะนำสำหรับการประยุกต์ใช้งานการเชื่อมต่อของอุปกรณ์อิเล็กทรอนิกส์กับเมืองอัจฉริยะ การขนส่งอัจฉริยะ และเทคโนโลยีที่มีความจำเป็นสำหรับโครงข่าย 5G ด้วย ไม่ว่าจะเป็นการรักษาความมั่นคงปลอดภัยในเทคโนโลยีเครือข่ายที่กำหนดโดยซอฟต์แวร์ และเทคโนโลยีการจำลองเสมือนฟังก์ชันเครือข่าย โดยผู้สนใจสามารถค้นคว้าเพิ่มเติมเกี่ยวกับข้อแนะนำหรือมาตรฐานที่สำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของ 5G ได้จาก ITU-T (2015; 2016; 2017; 2018a; 2018b; 2018c)

ข้อแนะนำจากองค์กรอื่น ๆ

สมาพันธ์โครงข่ายโทรคมนาคมแบบเคลื่อนที่ยุคหน้า (Next Generation Mobile Network Alliance : NGMN) ได้เสนอแนะเกี่ยวกับข้อควรระวังและมาตรการด้านความมั่นคงปลอดภัยสำหรับโครงข่าย 5G (NGMN; 2015) ทั้งเรื่องความท้าทายด้านความมั่นคงปลอดภัยในการเข้าถึงเครือข่าย การโจมตีทางไซเบอร์กับผู้ใช้งานโครงข่าย 5G และการโจมตีโครงสร้างพื้นฐานของโครงข่าย อาจเกิดได้หลายรูปแบบ ดังปรากฏในภาพที่ 2 ดังนี้



ภาพที่ 2 จุดต่าง ๆ ที่มีความเสี่ยงในโครงข่าย 5G

Note. From "Security for 5G and Beyond" by Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M., 2019. IEEE Communications Surveys & Tutorials, 21(4), p. 3689

1. การสกัดกั้นการเชื่อมต่อภายในโครงข่าย (Illegal intercept) โดยผู้ไม่ประสงค์ดี ซึ่งอาจเกิดขึ้นบริเวณเครือข่ายปลายน้ำและเครือข่ายกลางน้ำ 5G

2. การโจมตีด้วยการปฏิเสธการให้บริการ (Denial-of-service attacks) ซึ่งผู้ไม่ประสงค์ดีอาจโจมตีโครงข่าย 5G ด้วยการทำให้ระบบประมวลผลที่อยู่บนกลุ่มเมฆต่าง ๆ เช่น กลุ่มเมฆเครือข่ายสำหรับเครือข่ายต้นน้ำ 5G และกลุ่มเมฆชายขอบแบบเคลื่อนที่ไม่สามารถให้บริการได้

3. การจราจรข้อมูลที่เกิดขึ้นอย่างรวดเร็ว (Flash traffic) อาจเกิดจากการเชื่อมต่อของอุปกรณ์ IoT จำนวนมหาศาลกับโครงข่าย 5G ผ่านเครือข่ายปลายน้ำ แล้วอาจทำให้เกิดการเพิ่มขึ้นของการจราจรข้อมูลปริมาณมหาศาลในบางช่วงเวลา จนระบบไม่สามารถรองรับหรือให้บริการได้พร้อม ๆ กันทั้งหมด

4. การละเมิดความเป็นส่วนตัว (Privacy breach) ซึ่งอาจเกิดขึ้นกับผู้ใช้งานโครงข่าย 5G เช่น การโจมตีด้วยการดักฟังหรือดักจับข้อมูลของผู้ใช้งานเพื่อนำไปแสวงหาผลประโยชน์ในภายหลัง

5. สถานีฐานเท็จ (Fake BS) เป็นสถานีฐานที่ถูกจัดทำขึ้นโดยผู้ไม่ประสงค์ดีที่ต้องการหลอกให้ผู้ใช้งาน 5G ใช้อุปกรณ์ของตนเชื่อมต่อ ซึ่งวิธีนี้เกี่ยวข้องกับการดักจับเลขประจำตัวผู้เช่าเคลื่อนที่สากล (International Mobile Subscriber Identity: IMSI) และเป็นช่องทางในการโจมตีรูปแบบอื่น ๆ

6. การลักลอบใช้ทรัพยากร (Resource theft) อาจเป็นการลักลอบใช้ทรัพยากรที่สำคัญ ๆ เช่น ระบบประมวลผลที่มีอยู่ทั้งบนเครือข่ายต้นน้ำ 5G และเครือข่ายปลายน้ำ 5G รวมไปถึงอุปกรณ์เกตเวย์ (Gateway) ที่อยู่บนเครือข่ายกลางน้ำ 5G

7. ภัยคุกคามจากอินเทอร์เน็ต (Threats from internet) หมายถึง ภัยคุกคามทั่วไปที่พบบนเครือข่ายอินเทอร์เน็ต เช่น ไวรัสคอมพิวเตอร์ ซึ่งหากเครื่องแม่ข่ายต่าง ๆ ของโครงข่าย 5G ติดไวรัส อาจทำให้ข้อมูลในระบบเสียหาย หรือระบบไม่สามารถให้บริการได้ตามปกติ

8. ความขัดแย้งด้านนโยบายความมั่นคงปลอดภัย (Security policy conflicts) เป็นประเด็นที่อาจเกิดขึ้นในการโรมมิง (Roaming) และซึ่งจะต้องมีการรับส่งข้อมูลของผู้ใช้งานระหว่างผู้ให้บริการ และมีการแบ่งรายได้หรือผลประโยชน์ หากมีนโยบายไม่สอดคล้องกันก็อาจโรมมิงไม่ได้ ซึ่งจะส่งผลกระทบกับผู้ใช้งาน

เนื่องจากโครงข่าย 5G จะต้องมีความมั่นคงปลอดภัยสูงมากเพื่อป้องกันการโจมตีทางไซเบอร์ ดังนั้น ระบบรักษาความมั่นคงปลอดภัยควรมีความยืดหยุ่นสำหรับการทำงานร่วมกับเทคโนโลยีใหม่และการใช้การรักษาความปลอดภัยที่แตกต่างกัน เช่น การเข้ารหัส และด้วยเหตุที่ โครงข่าย 5G จะต้องรองรับการใช้งานที่หลากหลาย อาจมีช่องโหว่ต่าง ๆ ในเครือข่าย จึงจำเป็นที่จะต้องออกแบบโครงข่าย 5G ให้มีความมั่นคงปลอดภัย และมีระบบรักษาความปลอดภัยอัตโนมัติที่สามารถทำงานได้อย่างชาญฉลาดและสามารถปรับตัวเองตามสภาพแวดล้อมและภัยคุกคามที่อาจมีขึ้น ซึ่งจะต้องมีการประสานและการจัดการด้านความมั่นคงปลอดภัยแบบองค์รวม

นอกจากสมาพันธ์โครงข่ายโทรคมนาคมแบบเคลื่อนที่ยุคหน้าแล้ว ยังมีคณะทำงานโครงการหุ้นส่วน 3G (3G Partnership Project: 3GPP) ซึ่งเป็นสมาคมที่ทำหน้าที่กำหนดมาตรฐานสำหรับเทคโนโลยีโทรศัพท์เคลื่อนที่ ที่ผู้ผลิตจะต้องนำไปใช้ในการพัฒนาผลิตภัณฑ์ที่เกี่ยวข้องกับเทคโนโลยีโทรศัพท์เคลื่อนที่ ยังได้กำหนดมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับโครงข่าย 5G เอาไว้ด้วย โดยองค์กรนี้ได้ออกมาตรฐาน 3GPP TS 33.501 ออกมาหลายเวอร์ชัน เช่น 3GPP (2020a; 2020b) และได้กำหนดมาตรฐานสำหรับโครงข่าย 5G ไว้หลายประเด็น เช่น การกำหนดขอบข่ายงาน (Framework) สำหรับการยืนยันตัวตนแบบใหม่ที่จะต้องรองรับโพรโทคอลยืนยันตัวตนแบบขยาย (Extensible Authentication Protocol: EAP) ซึ่งมีความยืดหยุ่นแต่ปลอดภัย สามารถใช้ข้อมูลที่นอกเหนือจากที่มีการใช้งานทั่วไปในเครือข่ายโทรศัพท์เคลื่อนที่เพื่อรับรองหรือช่วยในการยืนยันตัวตนได้ ทำให้อุปกรณ์ตลอดจนบริการที่ไม่ได้เกี่ยวข้องกับการสื่อสารโทรคมนาคมโดยตรงก็สามารถเชื่อมต่อหรือใช้งานโครงข่าย 5G ได้

มาตรฐานของคณะทำงานโครงการหุ้นส่วน 3G สำหรับโครงข่าย 5G สามารถช่วยปกป้องความเป็นส่วนตัว (Privacy) โดยเฉพาะอย่างยิ่งการโจมตีด้วยการดักฟังหรือดักจับข้อมูลด้วยสถานีฐานเท็จ ซึ่งยังไม่มีรายงานว่าสามารถทำได้ นอกจากนั้นมาตรฐานของคณะทำงานโครงการหุ้นส่วน 3G สำหรับโครงข่าย 5G ยังถูกกำหนด

ให้ใช้สถาปัตยกรรมแบบใหม่ซึ่งเป็นสถาปัตยกรรมที่อยู่บนฐานของบริการ ทำให้ต้องมีการป้องกันและรักษาความมั่นคงปลอดภัยในโพรโทคอลชั้นบน เช่น ชั้นแอปพลิเคชัน นอกจากนั้นแล้ว สถาปัตยกรรมแบบใหม่ยังได้กำหนดให้มีส่วนที่ทำหน้าที่จัดการด้านความมั่นคงปลอดภัยในกรณีที่มีการเชื่อมต่อโครงข่ายระหว่างผู้ให้บริการ

นอกจากทั้ง 3 องค์กรที่กล่าวมาแล้ว ยังมีอีกหลายองค์กรที่ได้ศึกษา กำหนดข้อแนะนำ และมาตรฐานสำหรับโครงข่าย 5G ไม่ว่าจะเป็น องค์กรความร่วมมือระหว่างรัฐและเอกชนด้านโครงสร้างพื้นฐาน 5G (The 5G Infrastructure Public-Private Partnership: 5G PPP) ที่มุ่งเน้นในประเด็นของสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ กลไกการยืนยันตัวตน และความเป็นส่วนตัวของผู้ใช้งาน คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force: IETF) มุ่งเน้นในประเด็นการแก้ไขปัญหาด้านความมั่นคงปลอดภัยสำหรับอุปกรณ์ IoT ที่คาดว่าจะมีการใช้งานกันอย่างมากมายมหาศาลบนโครงข่าย 5G ความเป็นส่วนตัวของผู้ใช้งาน และหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ของเครือข่าย สถาบันมาตรฐานโทรคมนาคมยุโรป (European Telecommunications Standards Institute: ETSI) เน้นประเด็นของสถาปัตยกรรมความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยสำหรับการจำลองเสมือนฟังก์ชันเครือข่าย (NFV) การรักษาความมั่นคงปลอดภัยสำหรับ การประมวลผลชายขอบกลุ่มเมฆแบบเข้าถึงหลายทาง (Multi-access Edge Computing: MEC) และความเป็นส่วนตัวผู้ใช้งาน และสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ของสหรัฐอเมริกาที่มุ่งเน้นในด้านการรักษาความมั่นคงปลอดภัยสำหรับ IoT (Ahmad et al., 2019, p. 3692)

ผลการศึกษา

ทั้งเครือข่ายต้นน้ำ 5G เครือข่ายกลางน้ำ 5G และเครือข่ายปลายน้ำ 5G ที่ประกอบกันเป็นโครงข่าย 5G ต่างก็มีความเสี่ยงต่อการถูกคุกคาม จึงกลายเป็นประเด็นที่ท้าทายและจำเป็นต้องหาแนวทางในการแก้ไขหากเกิดปัญหา ซึ่งสามารถอธิบายแยกตามเครือข่ายได้ ดังนี้ (Ahmad et al., 2019, pp. 3692-3697)

ภัยคุกคามบนเครือข่ายต้นน้ำ 5G

เนื่องจากเครือข่ายต้นน้ำ 5G เป็นเครือข่ายแกนกลางของโครงข่าย 5G ที่พัฒนาขึ้นบนพื้นฐานของเทคโนโลยีอินเทอร์เน็ต ซึ่งต้องอาศัยเทคโนโลยีการจำลองเสมือนฟังก์ชันเครือข่าย ที่กำหนดโดยซอฟต์แวร์และกลุ่มเมฆ ทำให้มีความเป็นพลวัตสูง จึงอาจเป็นเป้าหมายหลักที่จะถูกคุกคามหรือโจมตีผ่านอุปกรณ์จำนวนมากที่เชื่อมต่อกับเครือข่ายต้นน้ำ 5G นอกจากนี้ยังรองรับอุปกรณ์ ตลอดจนบริการต่าง ๆ หลากหลายชนิดขึ้น โดยเฉพาะอุปกรณ์ IoT ทำให้มีการจราจรของข้อมูลประเภทต่าง ๆ เพิ่มสูงขึ้นมาก ซึ่งรวมถึงข้อมูลประเภทสัญญาณ (Signaling) ด้วย และหากการจราจรของข้อมูลประเภทนี้มีปริมาณสูงมากก็อาจทำให้เครือข่ายต้นน้ำ 5G ล่มได้

เพื่อแก้ปัญหาเหล่านั้นที่อาจเกิดขึ้น จึงมีการพัฒนาคุณสมบัติใหม่ ๆ ได้แก่

1. การแยกระนาบของผู้ใช้กับระนาบของผู้ควบคุม (Control-user plane)
2. การแบ่งส่วนเครือข่าย (Network slicing)
3. มีสถาปัตยกรรมฐานบริการ (Service based architecture)
4. มีความยืดหยุ่นในการเชื่อมต่อกับอุปกรณ์เครือข่ายที่หลากหลาย

สำหรับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับเครือข่ายต้นน้ำ 5G มีดังนี้

1. การโจมตีด้วยการปฏิเสธการให้บริการ (DoS attacks) ซึ่งอาจเป็นการโจมตีระบบที่ทำหน้าที่ดูแลระนาบสัญญาณ (Signaling plane) ซึ่งเป็นส่วนหนึ่งของระบบควบคุม
2. การส่งสัญญาณแบบพายุ (Signaling storms) อาจเป็นการระดมส่งสัญญาณระบบบางอย่าง เช่น สัญญาณเพื่อขอเชื่อมต่อกับระบบพร้อม ๆ กัน เช่น จากอุปกรณ์ IoT โดยมุ่งเน้นโจมตีอุปกรณ์ที่อยู่ในเครือข่ายต้นน้ำ 5G
3. การโจมตีแบบอิ่มตัว (Saturation attacks) ใช้โจมตีส่วนที่จัดการเกี่ยวกับอุปกรณ์เคลื่อนที่ (Mobility Management Entity: MME) ที่มีทรัพยากรในการประมวลผลจำกัด
4. การโจมตีแบบเจาะเข้าระบบ (Penetration attacks) เป็นรูปแบบที่นักเจาะระบบเครือข่ายคอมพิวเตอร์ หรือแฮกเกอร์ (Hacker) ใช้เพื่อวัตถุประสงค์บางอย่าง เช่น ขโมยข้อมูลของผู้ใช้งานทั้งหมดที่เชื่อมต่อกับระบบ
5. การขโมยรหัสประจำตัวผู้ใช้งาน (User identity theft) เพื่อใช้ในการเข้าถึงระบบและฐานข้อมูลของผู้ใช้งาน
6. การดักฟัง (Eavesdropping) เป็นรูปแบบของการดักฟังผ่านช่องทางควบคุม (Control channels) ของ 5GC
7. การเกิดความคับคั่งของการจราจรข้อมูลชั่วขณะจากอุปกรณ์ IoT (Traffic bursts by IoT) เป็นปัญหาที่เกิดจากการรับส่งข้อมูลพร้อม ๆ กันของอุปกรณ์ IoT ในปริมาณมหาศาล

ภัยคุกคามบนเครือข่ายกลางน้ำ 5G

สำหรับเครือข่ายกลางน้ำ 5G เมื่อมีอุปกรณ์ IoT จำนวนมากส่งสัญญาณข้อมูลปริมาณน้อยผ่านเครือข่ายเป็นระยะ ๆ อย่างต่อเนื่อง อาจทำให้เกิดปัญหากับอุปกรณ์บนเครือข่ายกลางน้ำ 5G จนเกิดการปฏิเสธการให้บริการได้ อย่างไรก็ตาม ด้วยความสามารถของเทคโนโลยี เครือข่ายที่กำหนดโดยซอฟต์แวร์ สามารถช่วยบริหาร

จัดการเครือข่ายกลางน้ำและช่วยจัดการกับปัญหาด้านความมั่นคงปลอดภัยได้ง่ายขึ้น เนื่องจากสามารถแยกระนาบของระบบควบคุม (Control plane) กับระนาบของข้อมูล (Data plane) ออกจากกันได้ อย่างไรก็ตาม ด้วยคุณลักษณะที่เครือข่ายกลางน้ำเป็นส่วนหนึ่งของโครงข่าย 5G โดยอยู่กลางระหว่างเครือข่ายต้นน้ำกับเครือข่ายปลายน้ำ 5G ดังนั้นเครือข่ายกลางน้ำ 5G จึงมีภัยคุกคามด้านความมั่นคงปลอดภัยน้อยเมื่อเทียบกับเครือข่ายต้นน้ำและเครือข่ายปลายน้ำ 5G

สำหรับการรับส่งข้อมูลทางอินเทอร์เน็ตหรือเครือข่ายภายนอก จะมีการส่งข้อมูลจากสถานีฐานไปยังเกตเวย์ที่ให้บริการ จากนั้นเกตเวย์ดังกล่าวจะส่งข้อมูลไปยังเกตเวย์เครือข่ายข้อมูลสาธารณะ (Public Data Network : PDN) ซึ่งการสื่อสารกับเครือข่ายภายนอกจะมีช่วงที่การใช้งานโพรโทคอลด้านความมั่นคงปลอดภัยที่ชื่อว่าโพรโทคอลจีทีพี (GPRS Tunneling Protocol: GTP) นอกจากนี้ยังสามารถประยุกต์ใช้โพรโทคอลไอพีเซ็ค (Internet Protocol Security: IPSec) ได้ด้วย เพื่อความปลอดภัยของข้อมูล

แม้ว่าเครือข่ายกลางน้ำ 5G จะมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ต่ำเมื่อเทียบกับเครือข่ายต้นน้ำและเครือข่ายปลายน้ำ 5G แต่ภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นได้ มีดังนี้

1. การโจมตีด้วยการดักชิงข้อมูล (Hijacking attacks) ซึ่งมีเป้าหมายในการโจมตีอาจเป็นส่วนควบคุมเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN controller) ที่อยู่บนเครือข่ายปลายน้ำ 5G
2. การโจมตีระดับทีซีพี (TCP level attacks) อาจเกิดขึ้นในรูปแบบของการที่ทำให้เกิดความคับคั่งของการจราจรข้อมูลในช่องทางการรับส่งข้อมูลบนชั้นการส่งข้อมูล (Transport layer)
3. การเกิดความคับคั่งของการจราจรข้อมูลชั่วขณะจากอุปกรณ์ IoT ที่เกิดจากการรับส่งข้อมูลพร้อม ๆ กันของอุปกรณ์เหล่านั้นในปริมาณมาก ๆ แม้ว่าปัญหานี้อาจจะไม่ได้เกิดจากความจงใจของผู้ไม่ประสงค์ดี แต่ก็ถือเป็นภัยคุกคามต่อโครงข่าย 5G รูปแบบหนึ่ง

ภัยคุกคามบนเครือข่ายปลายน้ำ 5G

เนื่องจากเครือข่ายปลายน้ำ 5G เป็นเครือข่ายแบบหลายชั้นที่ผสมผสานเทคโนโลยีไร้สายแบบต่าง ๆ ที่มีสถานีฐานขนาดเล็กจำนวนมากและมีความแตกต่างกันที่ติดตั้งอยู่ในบริเวณเดียวกันหรือใกล้เคียงกัน จึงอาจเกิดปัญหาสัญญาณรบกวนกันได้ ดังนั้น เครือข่ายปลายน้ำ 5G ที่ดี จำเป็นต้องมีกลไกในการแก้ปัญหาสัญญาณรบกวนที่ดีด้วย โดยสิ่งที่ผู้พัฒนาระบบโครงข่าย 5G และผู้วางระบบจำต้องพิจารณาคือเรื่องการเพิ่มความจุของเครือข่ายด้วยการติดตั้งสถานีฐานขนาดเล็กจำนวนมาก เพราะทำให้เพิ่มความเสี่ยงที่แฮกเกอร์อาจดักฟัง หรือมีผู้ใช้งานที่ไม่ได้รับอนุญาตแอบเชื่อมต่อระบบหรือเครือข่ายได้ นอกจากนี้ ในกรณีของสถานีฐานขนาดเล็ก ๆ ซึ่งจำเป็นต้องใช้พลังงานน้อย หากมีการลดการประมวลของอุปกรณ์ลงด้วยลดการตรวจสอบการเข้ารหัสข้อมูลก็จะกลายเป็นช่องโหว่ให้เกิดการโจมตีได้

สำหรับภัยคุกคามเครือข่ายปลายน้ำ 5G พบว่ามีภัยคุกคามบางอย่างที่เกิดขึ้นได้กับเครือข่ายต้นน้ำและเครือข่ายกลางน้ำ 5G แล้ว ยังเกิดขึ้นกับเครือข่ายปลายน้ำ 5G ได้ด้วย เช่น การโจมตีแบบอิ่มตัว การโจมตีด้วยการดักจับข้อมูล และการดักฟัง นอกจากนี้ ยังมีภัยคุกคามรูปแบบอื่น ๆ ที่สามารถส่งผลกระทบเชิงลบต่อเครือข่ายปลายน้ำ 5G ได้ ดังนี้

1. การเข้าถึงเครือข่ายโดยที่ไม่ได้รับอนุญาต (Un-authorized Access) เป็นการลักลอบเข้าใช้งานระบบอุปกรณ์เครือข่าย โดยปราศจากสิทธิ์หรือการขออนุญาต

2. การโจมตีค่าที่กำหนดไว้ในระบบ (Configuration attacks) เป็นการโจมตีด้วยการลักลอบเปลี่ยนแปลงค่าพารามิเตอร์ในอุปกรณ์เครือข่ายเพื่อวัตถุประสงค์บางอย่าง ซึ่งอาจเข้าไปเปลี่ยนแปลงได้โดยใช้รหัสผ่านที่กำหนดจากผู้ผลิตอุปกรณ์

3. การโจมตีแบบแบบแทรกกลางการสื่อสาร (Man-in-the-Middle : MITM) คือการที่แฮกเกอร์เข้ามาแทรกกลางในการสนทนาระหว่างคน 2 คนหรือเครื่องลูกข่ายกับแม่ข่าย แล้วเป็นตัวกลางในการรับส่งข้อมูลของทั้งสองฝั่ง จึงดักจับหรือเปลี่ยนแปลงข้อมูลได้

4. การเปิดรับคีย์ (Key exposure) เป็นรูปแบบของการดักจับเอนคริปชันคีย์ (Encryption key) ที่อาจจะถูกส่งผ่านช่องทางที่ไม่มีการเข้ารหัส เพื่อใช้ลักลอบเข้าระบบ

5. การโจมตีด้วยการเล่นซ้ำเซสชัน (Session replay attacks) เป็นรูปแบบการโจมตีระบบด้วยการนำเซสชันคีย์เก่ามาใช้ในการเข้าถึงเครือข่ายแบบ non-3GPP

6. การโจมตีด้วยการรีเซตและการปลอมแปลงไอพีแอดเดรส (Reset and IP spoofing) เป็นรูปแบบการปลอมแปลงไอพีเพื่อเข้าสู่ระบบ โดยอาศัยช่องโหว่ที่มีการตรวจสอบสิทธิ์เพียงครั้งเดียว

7. การโจมตีด้วยการสแกน (Scanning attacks) เป็นการสแกนหาพอร์ต (Port) ที่ถูกเปิดไว้ เพื่อหาทางเจาะเพื่อเชื่อมต่อเครือข่ายผ่านพอร์ตนั้น

8. การโจมตีด้วยการดักจับเลขประจำตัวผู้เช่าเคลื่อนที่สากล (IMSI catching attacks) เป็นการโจมตีด้วยการดักจับเลขประจำตัวที่ใช้ในการโรมมิง (Roaming) หรือใช้ในการเชื่อมต่อข้ามเครือข่าย ซึ่งผู้ไม่หวังดีสามารถนำไปใช้ในการลักลอบเชื่อมต่อกับเครือข่ายได้

9. การโจมตีด้วยการส่งสัญญาณรบกวน (Jamming attacks) เป็นการส่งสัญญาณรบกวนด้วยย่านความถี่เดียวกัน เพื่อไม่ให้อุปกรณ์สื่อสารไร้สายเชื่อมต่อกับสถานีฐานได้

อภิปรายผล ข้อสรุป และข้อเสนอแนะ

5G เป็นเทคโนโลยีหรือระบบสื่อสารโทรคมนาคมที่สามารถรองรับความต้องการและการใช้งานที่เพิ่มขึ้นเป็นอย่างมาก สามารถประยุกต์ใช้งานได้อย่างหลากหลายและมีประสิทธิภาพ เช่น การพัฒนาระบบการแพทย์และสาธารณสุขดิจิทัล (E-Health) และการเพิ่มประสิทธิภาพให้กับการประมวลผลชายขอบกลุ่มเมฆ (Edge computing) (พีระพงษ์ มานะกิจ, 2562, น. 30; ไพโรจน์ ไววานิชกิจ, 2562, น. 318) โดยเฉพาะอย่างยิ่งเมื่อเกิดการระบาดของโรคไวรัสโควิด-19 (COVID-19) ที่ทำให้พนักงานและเจ้าหน้าที่ในหลายภาคส่วนจำเป็นต้องทำงานจากที่บ้าน (Work from home) รวมทั้งนักเรียนนักศึกษาบางส่วนต้องเรียนผ่านระบบออนไลน์ (E-learning) ซึ่งรูปแบบชีวิตที่เปลี่ยนแปลงนี้ อาจนำไปสู่การดำเนินชีวิตวิถีใหม่ (New normal) ที่ต้องพึ่งพาอาศัยการสื่อสารโทรคมนาคมและเทคโนโลยีสารสนเทศและดิจิทัลมากยิ่งขึ้น (WHO, 2020; มูลนิธิการศึกษาทางไกลผ่านดาวเทียม, 2563; จุฬาลงกรณ์มหาวิทยาลัย, 2563)

จากหัวข้อต่าง ๆ ที่อธิบายในบทความนี้แสดงประเด็นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์สำหรับ 5G ซึ่งเป็นระบบการสื่อสารโทรคมนาคมขนาดใหญ่ที่ประกอบด้วยเครือข่ายต้นน้ำ 5G เครือข่ายกลางน้ำ 5G และเครือข่ายปลายน้ำ 5G ที่ถูกพัฒนาขึ้นโดยอาศัยเทคโนโลยีที่เกี่ยวข้องอื่น ๆ เช่น NFV และ SDN ตลอดจนเทคโนโลยี Cloud, Massive MIMO และเทคโนโลยีอื่น ๆ ทำให้เกิดเป็นช่องโหว่หรือช่องทางให้ผู้ไม่หวังดีโจมตีได้ รวมไปถึงปัญหาที่อาจเกิดขึ้นในระบบเองเมื่อต้องรองรับการจราจรข้อมูลในปริมาณมหาศาล ซึ่งสิ่งเหล่านี้ล้วนเป็นปัญหาด้านความมั่นคงปลอดภัยไซเบอร์สำหรับ 5G

ดังนั้นประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์สำหรับโครงข่าย 5G ที่เริ่มมีการใช้งานแล้วในประเทศไทยและจะกลายเป็นโครงสร้างพื้นฐานที่สำคัญของประเทศในอนาคต จึงกลายเป็นเรื่องที่สำคัญไม่ยิ่งหย่อนไปกว่าประเด็นเรื่องสมรรถนะ ประสิทธิภาพ และการประยุกต์ใช้งาน 5G ในบริบทต่าง ๆ โดยเฉพาะอย่างยิ่ง วิศวกรผู้ดูแลโครงข่าย 5G ในอนาคตอันใกล้ จะต้องเป็นผู้ที่มีความตระหนักและมีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับที่ดี นอกเหนือจากความรู้ความสามารถด้านเครือข่ายสื่อสารข้อมูล และความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารซึ่งถือเป็นความรู้ความสามารถพื้นฐานของผู้ดูแลโครงข่ายสื่อสาร นอกจากนี้ ผู้ให้บริการระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายคอมพิวเตอร์และการสื่อสารข้อมูลยังสามารถนำประเด็นด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงข่าย 5G ไปพัฒนาบุคลากรเพื่อเตรียมความพร้อมในการแข่งขันและพัฒนาธุรกิจในอนาคตได้ รวมไปถึงสถาบันการศึกษาต่าง ๆ ที่อาจพิจารณาปรับปรุงหลักสูตรและเนื้อหาวิชาที่เกี่ยวกับความมั่นคงปลอดภัยสำหรับเครือข่ายให้สอดคล้องกับเทคโนโลยี 5G เพื่อเพิ่มโอกาสในการได้งานของบัณฑิต

อย่างไรก็ดี แม้บทความนี้จะพยายามอธิบายให้ครอบคลุมเนื้อหาที่สำคัญด้านความมั่นคงปลอดภัยไซเบอร์สำหรับ 5G แต่ก็ทำได้เพียงบางส่วนเท่านั้น ยังมีอีกหลายประเด็นที่ยังไม่ได้กล่าวไว้ในบทความนี้ เช่น ประเด็นเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับโครงข่าย 5G ซึ่งเป็นประเด็นใหม่ที่เกี่ยวข้องกับผู้ใช้งานทั่วไปโดยตรง จึงควรมีการนำเสนอประเด็นเหล่านี้เพิ่มเติมในบทความต่อไป

บรรณานุกรม

กสทช. (2563). ประมูล 5จี สุดคึกคักจบการประมูลเงินรวม 100,521 ล้านบาท. ค้นเมื่อ 10 มิถุนายน 2563 จาก https://www.nbtc.go.th/News/Press-Center/40150.aspx.

จุฬาลงกรณ์มหาวิทยาลัย. (2563). นักวิชาการจุฬาฯ เสนอแนวทางรับมือ New Normal ภายหลังวิกฤตโควิด-19. ค้นเมื่อ 10 มิถุนายน 2563 จาก https://www.chula.ac.th/news/30432/.

เทอดพงษ์ แดงสี และ พิสิฐ พรพงศ์เตชวาณิช. (2562). 5G: เทคโนโลยีการสื่อสารแห่งทศวรรษหน้า. *วารสารวิชาการเทคโนโลยีอุตสาหกรรม,* 15(2), 167-197.

ผู้จัดการออนไลน์. (2563). ทรูมูฟ เอช เริ่มเปิดให้บริการ 5G อย่างเป็นทางการในพื้นที่กรุงเทพฯ ชั้นใน. ค้นเมื่อ 10 มิถุนายน 2563 จาก https://mgronline.com/cyberbiz/detail/9630000027049.

พีระพงษ์ มานะกิจ. (2562). กสทช. กับการประยุกต์ใช้เทคโนโลยี 5G เพื่อประโยชน์ทางการแพทย์. *วารสารวิชาการ กสทช.*, 4, 29-41.

ไพโรจน์ ไววานิชกิจ. (2562). 10 เทคโนโลยีดิจิทัลใหม่สำหรับโลกธุรกิจ 2562. *วารสารวิชาการ กสทช.*, 4, 307-327.

มูลนิธิการศึกษาทางไกลผ่านดาวเทียม. (2563). 6 ช่องทางการรับชมการเรียนการสอนทางไกลผ่านดาวเทียม ในสถานการณ์การแพร่ระบาดของเชื้อไวรัส COVID-19. ค้นเมื่อ 10 มิถุนายน 2563 จาก https://www.dltv.ac.th/content/content-detail/10537/1001.

ราชกิจจานุเบกษา. (2562). พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. ค้นเมื่อ 1 มิถุนายน 2563 จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

วิชัย โชควิวัฒน. (2562). สงครามไซเบอร์. *วารสารวิชาการ กสทช.*, 4, 351-356.

วิเชียร ปรีดาลัมพะบุตร. (2563). แนะนำและสาธิตการทดสอบการใช้งานเทคโนโลยีเปลี่ยนโลกอย่างง่าย: กรณีศึกษาโครงข่ายที่ถูกกำหนดหน้าที่การทำงานโดยซอฟต์แวร์ (เอสดีเอ็น). *วารสารวิชาการ กสทช.*, 4, 219-237.

สพร. (2559). ความมั่นคงปลอดภัยทางไซเบอร์. ค้นเมื่อ 20 พฤษภาคม 2563 จาก https://dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf.

3GPP. (2020a). Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.7.0 Release 15). Retrieved May 20, 2020 from https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.07.00_60/ts_133501v150700p.pdf.

____. (2020b). Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.8.0 Release 15). Retrieved May 20, 2020 from https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.08.00_60/ts_133501v150800p.pdf.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials*, 21(4), 3682-3722. doi: 10.1109/COMST.2019.2916180.

Bendale, S. P. & Prasad J. R. (2018). Security Threats and Challenges in Future Mobile Wireless Networks. 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 146-150.

Fang, D., Qian, Y., & Hu, R. Q. (2018). Security for 5G Mobile Wireless Networks. *IEEE Access,* 6(2), 4850-4874. doi: 10.1109/ACCESS.2017.2779146.

GSMA. (2019). Mobile Backhaul: An Overview. Retrieved August 24, 2020 from https://www.gsma.com/futurenetworks/wiki/mobile-backhaul-an-overview/

Huawei. (2017). Service-Oriented 5G Core Networks [White Paper]. Retrieved May 20, 2020 from https://carrier.huawei.com/~/media/CNBG/Downloads/track/HeavyReadingWhitepaperServiceOriented5GCoreNetworks.pdf.

ITU-T. (2008). ITU-T X.1205: Overview of cybersecurity. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

_____. (2015). ITU-T X.1601: Security framework for cloud computing. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1601-201510-I!!PDF-E&type=items.

_____. (2016). ITU-T X.1038: Security requirements and reference architecture for software-defined networking. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1038-201610-I!!PDF-E&type=items.

_____. (2017). ITU-T X.1362: Simple encryption procedure for Internet of things (IoT) environments. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1362-201703-I!!PDF-E&type=items.

_____. (2018a). ITU-T Y.3102: Framework of the IMT-2020 network. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3102-201805-I!!PDF-E&type=items.

_____. (2018b). ITU-T X.1361: Security framework for the Internet of things based on the gateway model. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1361-201809-I!!PDF-E&type=items.

_____. (2018c). ITU-T Y.2323: Requirements and capabilities of orchestration in next generation network evolution. Retrieved May 20, 2020 from https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-Y.2323-201812-I!!PDF-E&type=items.

NGMN. (2015). NGMN 5G White Paper [White Paper]. Retrieved May 20, 2020 from https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf.

Techsauce. (2563). AIS เริ่มให้บริการ 5G ในประเทศไทยพร้อมปักหมุดครอบคลุมแหล่งชุมชนและย่านสำคัญ. ค้นเมื่อ 10 มิถุนายน 2563 จาก https://techsauce.co/pr-news/ais-5g-mobile-commercial-internet-wifi.

Vani, B. P., & Sundaraguru, R. (2019). Insights on Significant Implication on Research Approach for Enhancing 5G Network System. *Indonesian Journal of Electrical Engineering and Informatics*, 7(3), 586-598.

WHO. (2020). Rolling updates on coronavirus disease (COVID-19) [Website]. Retrieved June 10, 2020 from https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.