Lightweight Denial of Service (DOS) Detection System Algorithm (LIDSA)

Abdul Fuad Abdul Rahman[1], Azni Ab Halim[2], Shazwani Salleh[3], Nur Farahin Jamaludin[4], Nurul Syazwani Kamarulzaman[5], Madihah Zulfa Mohamad[6]

[13456]MyVAC Department, CyberSecurity Malaysia, Cyberjaya, Malaysia

[2]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Malaysia

abdulfuadrahman@gmail.com, ahazni@usim.edu.my, shazwani.salleh@cybersecurity.my, nurfarahin@cybersecurity.my, nurul.syazwani@cybersecurity.my, madihah@cybersecurity.my

***Abstract*—The Internet of Things (IoT) is becoming an increasingly growing topic. IoT encompasses everything connected to the internet. IoT requires multi-facet security solutions where the communication is secured with confidentiality, integrity, and availability of the service. However, IoT Sensor Node has the requirement to minimize power usage and computational power due to the requirement to be miniature. Therefore, the challenge of implementing security in the IoT Sensor Node must be addressed. Even if the IoT Sensor Node is protected with encryption and authentication, the protection is not comprehensive to sustain a Denial of Service (DoS) attack. The DoS attack is considered one of the security threats that may affect IoT network's quality service and reduce the lifespan of IoT Sensor Node. Hence, mitigation shall be needed to secure IoT Sensor Node. The objective of this paper is to propose a lightweight Denial of Service (DoS) Detection Systems algorithm to secure IoT Sensor Node. The approach uses data from previous experiments and translated it to develop mitigation to secure IoT Sensor Node, thus increasing the lifespan of IoT Sensor Node.**

***Keyword*— Denial of Service, Internet of Things, Detection System, Lightweight, Sensor Node**

Abdul Fuad Abdul Rahman, is a the Head of Malaysia Vulnerability Assessment Centre (MyVAC) of CyberSecurity Malaysia. Prior to th at, he has a System Security Certified Practitioner (SSCP) from The International Information Systems Security Certification Consortium (ISC)2, GIAC Assessing Wireless Network (GAWN) from SANS Institute of America and Certified Network Engineer IPv6 (CNE6).

Azni Ab Halim is the Deputy Dean of Postgraduate Centre of Studies of Universiti Sains Islam Malaysia (USIM). She has a Doctorate Degree in the field of ICT from the Universiti Teknikal Malaysia Melaka (UTeM) in 2012. She is currently focusing her research works in the field of ICT security.

Shazwani Salleh is an Analyst at CyberSecurity Malaysia in Cyberjaya where she is involved in Research and Development (R&D) for Internet of Things (IoT) projects as well as Vulnerability Assessment and Penetration Testing (VAPT) services.. She received her Bachelor of Science (B.Sc), in field of Business Computing, from Universiti Teknologi Mara (UiTM), Malaysia, in 2015. She completed her Master of Science (Msc), in field of Information Management, from Universiti Teknologi Mara (UiTM) in 2016. In 2017, she started her career as Associate Analyst at DHL Asia Pacific IT Services.

Farahin Jamaludin is an Analyst at CyberSecurity Malaysia in Cyberjaya where she is involved in Research and Development (R&D) for Internet of Things (IoT) projects as well as Vulnerability Assessment and Penetration Testing (VAPT) services. She received her Bachelor's Degree in the field of Engineering Technology (Manufacturing), from Universiti Malaysia Pahang, Malaysia, in 2019.

Nurul Syazwani Kamarulzaman is an Analyst at Malaysia Vulnerability Assessment Center (MyVAC) department where she is involved in Vulnerability Assessment Penetration Testing (VAPT) and Research and Development (R&D) for Internet of Things (IoT). She received her Bachelor's Degree in the field of Science Computer (Network Security), from University Sultan Zainal Abidin (UniSZA), Terengganu Malaysia in 2016.

Madihah Zulfa Mohamad, a Manager with the CyberSecurity Malaysia. Prior to that, she has a Certified Ethical Hacker (CEH) from EC-Council and Microsoft Certified System Engineer (MCSE) from Microsoft. She is currently focus in the research on the field of IoT and ICT Security.