Adaptive Anomaly Detection of CTS Flooding in Wi-Fi Networks Using Sketch-Based Profiling

Asif Hossain Joy, Zinadin Zidan, Nahar Sultana

Department of Computer Science, Faculty of Science and Technology, American International University - Bangladesh, Dhaka, Bangladesh

22-47850-2@student.aiub.edu, 22-47918-2@student.aiub.edu, nahar@aiub.edu

***Abstract*—Using Wi-fi in both public and private networks could be challenged by IEEE 802.11 MAC-layer protocol problems. This study concentrates on the Clear-to-Send (CTS) flood attack, characterized as a low-effort, high-impact threat that is significantly perilous and not widely recognized. This vulnerability "poisons" the Network Allocation Vector (NAV) of real devices by taking advantage of the fact that CTS control packets do not need to be checked. This weakness makes them silent for long periods of time and badly messes up communication. Today's intrusion detection systems (IDS) do not know about this issue since they focus on monitoring data and management frames. In addition, traditional rule-based protections also do not anymore work, which may be easily avoided by attackers. The proposed system learns the typical time, frequency, and length of the CTS traffic behavior, allowing it to identify anomalous changes. This paper offers a novel approach to detecting abnormalities employing sketch-based profiling to address significant security vulnerabilities. The proposed architecture offers a flexible and scalable solution to safeguard various Wi-Fi networks, ranging from public networks to corporate campuses, against an unidentified attack vector.**

***Keyword*—About CTS flooding, Anomaly Detection, Wi-Fi, Sketch-based Profiling**

Asif Hossain Joy is a final-year undergraduate student in the Department of Computer Science and Engineering at American International University-Bangladesh (AIUB) Dhaka, Bangladesh, where he is pursuing his B.Sc. degree in CSE. His academic and practical interests are focused on cybersecurity, with particular emphasis on network security, wireless security, intrusion detection systems, ethical hacking, and cyber-attack mitigation. He aims to build a professional career in cybersecurity and contribute to the development of secure, reliable, and resilient digital systems.

Zinadin Zidan is currently an undergraduate student in the Department of Computer Science and Engineering at American International University–Bangladesh (AIUB), Dhaka, Bangladesh, where he is pursuing his B.Sc. in Computer Science and Engineering (CSE). His interests include artificial intelligence, network security, wireless security, and healthcare-related computing applications. He is particularly interested in secure and intelligent system design and their practical applications in real-world environments.

Dr. Nahar Sultana is an Associate Professor in Department of Computer Science of American International University- Bangladesh (AIUB). She completed her Ph.D. from Green Networking Research Lab, Department of Computer Science and Engineering, University of Dhaka. She obtained M.Sc. degree from the Department of Computer Science and Engineering, Kyung Hee University, South Korea in the year 2008. Prior to that she received B.Sc degree in Department of Computer Engineering from American International University-Bangladesh (AIUB). Her research interest are IoT, NB-IoT, Healthcare, Wireless sensor network, Crowdsourcing, food delivery etc.