UNIVERSITI TEKNOLOGI MARA

DEDEPRO WIRELESS INTRUDER DETECTION SYSTEM (WIDS) AGAINST DE-AUTHENTICATION / DISASSOCIATION ATTACKS IN 802.11 A/B/G/N

NORZAIDI BIN BAHARUDIN

Dissertation submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Computer Networking

Faculty of Computer and Mathematical Science

July 2014

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

ABSTRACT

Wireless network is always being a target from the various kinds of attacks. Many kind of security mechanism were introduced, such as WEP, WPA and WPA2. However, this security mechanism is only to protect the network from the outside access. Those security mechanisms are not handle of the security and protection of the wireless clients that are vulnerable to the internal attacks such as contributed by the weakness of management frames on 802.11a/b/g/n. The management frames on 802.11a/b/g/n are sent unencrypted with a plain text, thus it can be spoof and forge by anybody on the area of the wireless proximity. Even though they was introduced the 802.11w that will protect the management frames but there are still lot of legacy wireless devices been used and not supported with 802.11w. The objective of this research is to propose a new kind of tools that can be use as a personal WIDS (Wireless Intruder Detection System). Furthermore, this research will introduce the detection mechanism of the de-authentication / disassociation attacks on current 802.11a/b/g/n. Finally, the result and analysis will be present and to show the effectiveness of the propose scheme.

CHAPTER 1
INTRODUCTION

1.0   OVERVIEW

This chapter explains the overview of the research work starting from the research background. The next subchapter is the problem statements that will discuss on the current limitation faced by 802.11 legacy devices. The next following will be the research questions that will be discuss details on this research. Next will be the research objectives that will answer the entire research question. After that, the scope of works involve in the research test bed. Then, the research significance and finally is the organization of the thesis.

1.1   RESEARCH BACKGROUND

Wireless technology has tremendous increasing rapidly. Public area are flooded with the Wi-Fi signal either at the schools or university, it's also can be found at any stalls, airports, private office, government office and even at small stall besides the road. The main contribution of the massive birth of Wi-Fi network also came from the ISP (Internet Service Provider) companies. Most of the ISPs are offered packages with including the Wi-Fi Technology that have been build-in in the broadband router modems. Other factors of the Wi-Fi technology rapidly increasing used is because of the gadgets that also have the capabilities of Wi-Fi such as mobile phone, tablet, smart TV, projector and also digital camera. Klasnja P. et.al (2009) reported a wireless networks lists over 16 million networks worldwide and that is likely a small fraction of the total number of Wi-Fi networks in use.

Malaysia government also has listed 6 focus areas on the National ICT Roadmap handbook including wireless intelligence and the security (MOSTI, 2014). The main concern about the Wireless Intelligence technologies is wireless data encryption besides wireless sensors, device interconnection, gestural interface, 3-D displays, RFID, Image recognition and data management system. The security technology main areas are IDS (Intruder Detection System), IPS (Intruder Prevention System), Next Generation Firewall and Data Encryptions. Thus, government realized