ABSTRACT

In recent years, wireless LAN systems are widely used in campuses, offices, homes and so on. It is important to discuss the security aspect of wireless LAN networks in order to protect data confidentiality and integrity. The IEEE Standards Association formulated some security protocols, for example, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access Temporal Key Integrity Protocol (WPA-TKIP). However, these protocols have vulnerability for secure communication. In 2008. We proposed an effective key recovery attack against WEP and it is called the TeAM-OK attack. In this paper, first, we present a different interpretation and the relation between other attacks and the TeAM-OK attack against WEP. Second, we present some existing attacks against WPA-TKIP and these attacks are not executable in a realistic environment. Then we propose an attack that is executable in a realistic environment against WPA-TKIP. This attack exploits the vulnerability implementation in the QoS packet processing feature of IEEE 802.11e. The receiver receives a falsification packet constructed as part of attack regardless of the setting of IEEE 802.11e. This vulnerability removes the attacker's condition that access points support IEEE 802.11e. We confirm that almost all wireless LAN implementations have this vulnerability. Therefore, almost all WPA-TKIP implementations cannot protect a system against the falsification attack in a realistic environment.

Basically, WEP and WPA are the major applications of **RC4** algorithm. **RC4** is the symmetric key encryption algorithm designed in 1987 by RSA(Ron Rivest, Adi Shamir and Leonard Adleman). It belongs to the category of stream cipher. While block ciphers operate on large blocks of data, stream ciphers typically operate on smaller units of plaintext, usually bits or bytes. A stream cipher generates what is called a key stream (a sequence of bits used as a key). **RC4** is especially **vulnerable** when the beginning of the output key-stream is not discarded, but **RC4**-dropN, being N a multiple of 256 is an improvement to solve this issue. It is also **vulnerable** when non-random or related keys are used, because it can lead to a very insecure system, such as WEP. Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic.