PAPER

, ??

SUMMARY Detecting a Rouge Access Point (RAP) in Wi-Fi network is imperative. The previous scheme is user side detection focusing on two channels used by a RAP. That scheme can detect a RAP in stable traffic environment by revealing the channel used with a Legitimate Access Point (LAP) with intentional interference. However, the detection performance is degraded in the real environment where traffic is more unstable because it affects the traffic on the channel. Thus, it is necessary to design the scheme which is independent of such factors. In this paper, we propose RAP detection by using Address Resolution Protocol (ARP) failure under the Media Access Control (MAC) address duplication. Our main idea is that the traffic is relayed via a RAP and a LAP on the LAN path between a client and a gateway under the attack. This is because the RAP must be established between a client and a LAP to provide Internet connection. On the basis of this idea, the proposed scheme reveals that the Access Point (AP) with whih a client connects is a RAP by discovering the MAC address of a LAP on the path. In order to find the MAC address, we leverage the phenomenon that a client cannot receive ARP reply packets in the situation where its MAC address and that of a AP are duplicated on the path. By doing this, the presence of a LAP is revealed, which can judge that the connected AP is a RAP. In our evaluation, the proposed scheme achieves accuracy of 96.5% even in unstable traffic environment. True positive rate and false positive rate are 31.0% higher and 9.0% lower than the previous scheme. Furthermore, the proposed scheme can detect RAPs accurately in real environment where the previous scheme cannot.

key words:

1.

References

[1]

Manuscript received January 1, 2015.
Manuscript revised January 1, 2015.
[†] The author is with the
DOI: 10.1587/trans.E0.??.1