URSI GASS 2023, Sapporo, Japan, 19 – 26 August 2023

Detection of Hidden Wireless Eavesdroppers based on their Backscattering Characteristics

Jie An(1), Zhendong Wang(1), and Qianyun Zhang* (1)
(1) Beihang University, Beijing, China; e-mail: zhangqianyun@buaa.edu.cn

In recent decades, wireless communication systems have significantly broadened the communication boundary and range, while signals propagating in the free space also expose these systems to eavesdropping attacks. Various encryption algorithms have been explored developed and deployed to improve the confidentiality of systems. However, these approaches increase the message size and communication delay, and a low-security level is realized for devices with limited computation ability [1]. Detection of eavesdroppers has attracted interest from both industry and academia since it provides an active countermeasure to eavesdropping attacks. Only receiving electromagnetic signals but never transmitting, the perception of hidden wireless eavesdroppers is quite challenging. Furthermore, with the development of integrated and miniaturized radio frequency (RF) circuits, these eavesdroppers are easily hidden in legal devices, and therefore disabling traditional detection techniques [2].

In this work, we proposed a hidden eavesdropper detection scheme based on backscattering characteristics of the eavesdropper antenna, which is a must component for wireless signal reception. From the antenna theory [3], the scattering field $\mathbf{E^s}$ from an antenna is a linear combination of two terms and written as

$$\mathbf{E^s}(Z_L) = \mathbf{E_0} + \frac{Z_L}{Z_L + Z_A}\mathbf{E^t}, \tag{1}$$

where $\mathbf{E_0}$ and $\mathbf{E^t}$ are the structure scattering field and radiation field, respectively. Z_A is the input impedance of the antenna, and Z_L is the loaded impedance at the excitation port. As the antenna is always connected to the RF front with active devices such as low-noise amplifiers (LNA) in modern receivers, Z_L can differ based on the DC power supply, as the resistance of transistors in LNA changes dramatically with or without DC basing. In this way, using the device under test (DUT) as a scatter, and controlling the power supply of DUT, the existence of a hidden eavesdropper can be justified by measuring and recording the back-scattered field from DUT. Full-wave numerical simulations have been carried out to verify the effectiveness of the proposed method. As a non-destructive detection scheme, the proposed method has no distance limit compared with those near field-based techniques such as the local oscillator leakage detection method.

References

[1] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review the International Journal of Technology & Practice, 26, 1, January 2010, pp. 23-30, doi: 10.1016/j.clsr.2009.11.008

[2] Y. Zou, J. Zhu, X. Wang, L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Proceedings of the IEEE, 104, 9, September 2016, pp. 1727-1765, doi:10.1109/JPROC.2016.2558521

[3] C. A. Balanis, "Antenna Theory: Analysis and Design, 4th Edition," John Wiley & Sons, February 2016, ISBN: 978-1-118-64206-1