

Chapter 2

Feasibility of Launching User Spoofing

We provide a brief overview of identity-based spoofing attack, and its impact to the wireless and sensor networks in this chapter.

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks, in particular, the most harmful but easy to launch attack: *spoofing attacks*.

In an user-spoofing attack, an attacker can forge its identity to masquerade as another device, or even creates illegitimate identities in the networks. For instance, in an 802.11 network, it is easy for an attacker to modify its MAC address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point or as an authorized client, an attacker can launch denial of service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients. The 802.11 protocol suite provides insufficient identity verification during message exchange, including most control and management frames. Therefore, the adversary can utilize this weakness and request various services as if it were another user. Identity-based spoofing attacks are a serious threat in the network since they represent a form of identity compromise and can facilitate a series of traffic injection attacks, including spoofing-based denial-of-service (DoS) attacks.

For instance, an adversary can launch a deauthentication attack. After a client chooses an access point for future communication, it must authenticate itself to the access point before the communication session starts. Both the client and the access point are allowed to explicitly request for deauthentication to void the existing authentication relationship with each other. Unfortunately, this deauthentication message is not authenticated. Therefore, an attacker can spoof this deauthentication message, either on behalf of the client, or on behalf of the access point [1, 2]. The adversary can persistently repeat this attack and completely prevent the client from transmitting or receiving.

Further, an attacker can utilize identity spoofing and launch the Rogue Access Point (AP) attack against the wireless network. In the Rogue AP attack, the adversary first sets up a rogue access point with the same MAC address and SSID as the

legitimate access point, but with a stronger signal. When a station enters the coverage of the rogue AP, the default network configuration will make the station automatically associate with the rogue access point, which has a stronger signal. Then the adversary can take actions to influence the communication. For example, it can direct fake traffic to the associated station or drop the requests made by the station. Besides the basic packet flooding attacks, the adversary can make use of identity-spoofing to perform more sophisticated flooding attacks on access points, such as probe request, authentication request, and association request flooding attacks [3].

Therefore, the identity-based spoofing attacks will significantly impact the network performance. The conventional approaches to address identity-based attacks use authentication. However, the application of authentication requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply authentication because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise—a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned.

Thus, it is desirable to use properties that do not require overheads and changes on nodes and cannot be undermined even when nodes are compromised. We propose to use Received Signal Strength (RSS), a property associated with the transmission and reception of communication (and hence not reliant on cryptography), as the basis for detecting identity-based attacks. Employing RSS as a means to detect spoofing attacks will not require any additional cost to the wireless devices themselves—they will merely use their existing communication methods, while the wireless network will use a collection of access points to monitor received signal strength for the potential of identity-based attacks. Our proposed techniques will handle the problem of unreliable and time-varying nature of RSS [4, 5]. These techniques will also address the issues when an attacker varies its transmission power to launch attacks and trick the system.

References

1. J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in *Proceedings of the USENIX Security Symposium*, 2003, pp. 15–28.
2. W. A. Arbaugh, N. Shankar, Y. Wan, and K. Zhang “Your 802.11 network has no clothes,” *IEEE Wireless Communications*, vol. 9, no. 6, pp. 44–51, Dec. 2002.
3. F. Ferreri, M. Bernaschi, and L. Valcamonici “Access points vulnerabilities to dos attacks in 802.11 networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2004.
4. G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, “Models and solutions for radio irregularity in wireless sensor networks,” *ACM Transactions on Sensor Networks*, vol. 2, pp. 221–262, 2006.
5. A. Krishnakumar and P. Krishnan, “On the accuracy of signal strength-based location estimation techniques,” in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2005.

Pervasive Wireless Environments: Detecting and
Localizing User Spoofing

Yang, J.; Chen, Y.; Trappe, W.; Cheng, J.

2014, VIII, 72 p. 27 illus., Softcover

ISBN: 978-3-319-07355-2