

**CHENNAI – PONDICHERRY**

**Authenticating Users through Fine-grained Channel Information**

**Abstract:**

User authentication is the critical first step in detecting identity-based attacks and preventing subsequent malicious attacks. However, the increasingly dynamic mobile environments make it harder to always apply cryptographic-based methods for user authentication due to their infrastructural and keymanagement overhead. Exploiting non-cryptographic based techniques grounded on physical layer properties to perform user authentication appears promising. In this work, the use of channel state information (CSI), which is available from off-the-shelf WiFi devices, to perform fine-grained user authentication is explored. Particularly, a user-authentication framework that can work with both stationary and mobile users is proposed. When the user is stationary, the proposed framework builds the user profile for user authentication which is resilient to the presence of a spoofer. The proposed machine learning based user-authentication techniques can distinguish between two users even when they possess similar signal fingerprints and detect the existence of the spoofer. When the user is mobile, it is proposed to detect the presence of the spoofer by examining the temporal correlation of CSI measurements. In both office building and apartment environments show that the proposed framework can filter out signal outliers and achieve higher authentication accuracy compared with existing approaches using received signal strength (RSS).

**Existing System:**

Authentication based on noncryptographic methods has been proposed to compliment and enhance the existing cryptography based schemes [3], [6], [10]. For example, channel based authentication schemes use the Received Signal Strength (RSS) of wireless packets or the Channel Impulse Response (CIR) of a single frequency to generate fingerprints of the wireless channel to perform user authentication.

The rationale behind these schemes is that both RSS and CIR present unique spatial properties due to path loss and multi-path effects. An adversary, situated at a different location from the legitimate user, will incur different RSS or CIR profiles. However, the RSS and CIR extracted from a single frequency only provide coarse-grained information about the wireless channel and thus the effectiveness of user authentication is largely limited. For example, the RSS-based authentication can hardly distinguish between two users with similar signal signatures even though they may be located far away from each other.

**Proposed System:**

We show that it is feasible to perform user authentication by utilizing CSI from OFDM even when the users possess similar signal fingerprints, making fine-grained user authentication achievable in practice.

We develop a user authentication framework that works with both stationary and mobile users. To deal with a stationary user, the proposed framework has the capability of building a user profile under the presence of a spoofing attack and achieves higher authentication accuracy compared with existing channel based (e.g., RSSbased) methods. For mobile users, the framework performs real-time user authentication by leveraging temporal correlation of CSI measurements.

We validate the framework by conducting real experiments in both office and apartment environments using off-the-shelf WiFi devices. Experimental results confirm that our framework is highly robust and effective in user authentication under various attacking scenarios without requiring any additional overhead on wireless devices.