Researchers at the University of South Florida have developed a novel way to prevent outsiders from gaining access to wireless signals by broadcasting a jamming signal during Cyclic Prefix (CP) durations.

Broadcast nature of wireless medium threatens the privacy and security of wireless communication. An eavesdropper can easily capture wireless signals even from a far location. In order to provide a secure communication under the presence of such threats, data protection techniques are crucial. Encryption based methods conventionally provide security; however, may not always protect the data against today's advanced attacks. Therefore, further security precautions gain more importance.

USF Inventors have found a novel way to prevent eavesdroppers from gaining access via wireless signals. Friendly CP jamming broadcasts a jamming signal to interfere with the signal the eavesdropper receives, which prevents him/her from decoding the information correctly. This is accomplished without requiring any complex processing and spectral resources as well as without causing a distortion in the signal of legitimate users. The technology performs jamming during the CP duration at the receiver side, independent of the remaining processes. Thus, the data part of adversaries can be distorted by jamming signal due to propagation delay by causing no interference on the legitimate receiver's data. The method adds a layer of security for any wireless signals, providing great benefits for Wi-Fi and telecommunication devices.

**ADVANTAGES:**
- Increased security for wireless signals
- Cyclic Prefix (CP) duration delay does not affect signal of legitimate user
- Does not require complex processing or spectral resources

**Preventing Outsiders from Accessing Signals While Causing no Distortion to Legitimate Users**

![Flowchart showing one functional arrangement where a jamming signal is broadcast for the CP duration](image)

The Flowchart Showing One Functional Arrangement Where a Jamming Signal is Broadcast for the CP Duration