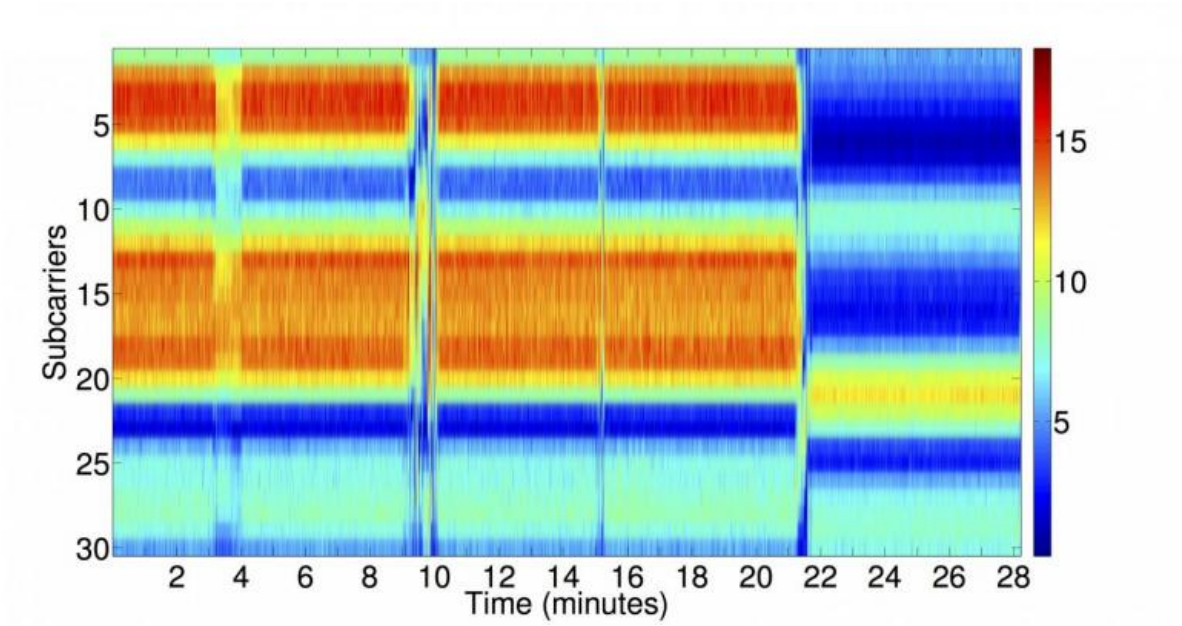
WiFi signals can be exploited to detect attackers

December 18 2015



Attached image: A visual representation of the phenomenon. At 10mins and 15mins a person is moving through the environment, while at 21mins the device is being tampered with.

Physical attacks on devices connected to the Internet can be detected by analysing WiFi signals, computer scientists have discovered.

Wireless devices are increasingly used for critical roles, such as security systems or industrial plant automation. Although wireless transmissions

can be encrypted to protect transmitted data, it is hard to determine if a device – such as a wirelessly connected security camera protecting critical buildings in airports or power stations – has been tampered with. An attacker may simply rotate a camera's view away from the area it is guarding without triggering an alert.

Researchers at Lancaster University, in their study 'Using Channel State Information for Tamper Detection in the Internet of Things' have created a method that analyses WiFi signals at multiple receivers to detect physical attacks. A change in the pattern of wireless signals – known as Channel State Information (CSI) – picked up by the receivers can indicate a tamper situation. The algorithm detects attacks despite signal noise caused by natural changes to the environment such as people walking through the communication paths.

Dr Utz Roedig, Reader in Lancaster University's School of Computing and Communications and one of the report's authors, said: "A large number of Internet of Things systems are using WiFi and many of these require a high level of security. This technique gives us a new way to introduce an additional layer of defence into our communication systems. Given that we use these systems around critically important infrastructure this additional protection is vital."

Provided by Lancaster University