UKRI Engineering and Physical Sciences Research Council
TOSHIBA
University of BRISTOL
ROKE
GCHQ

EPSRC Prosperity Partnership
SWAN (Secure Wireless Agile Networks)
Grant Reference: EP/T005572/1

Radio Frequency Vulnerabilities White Paper

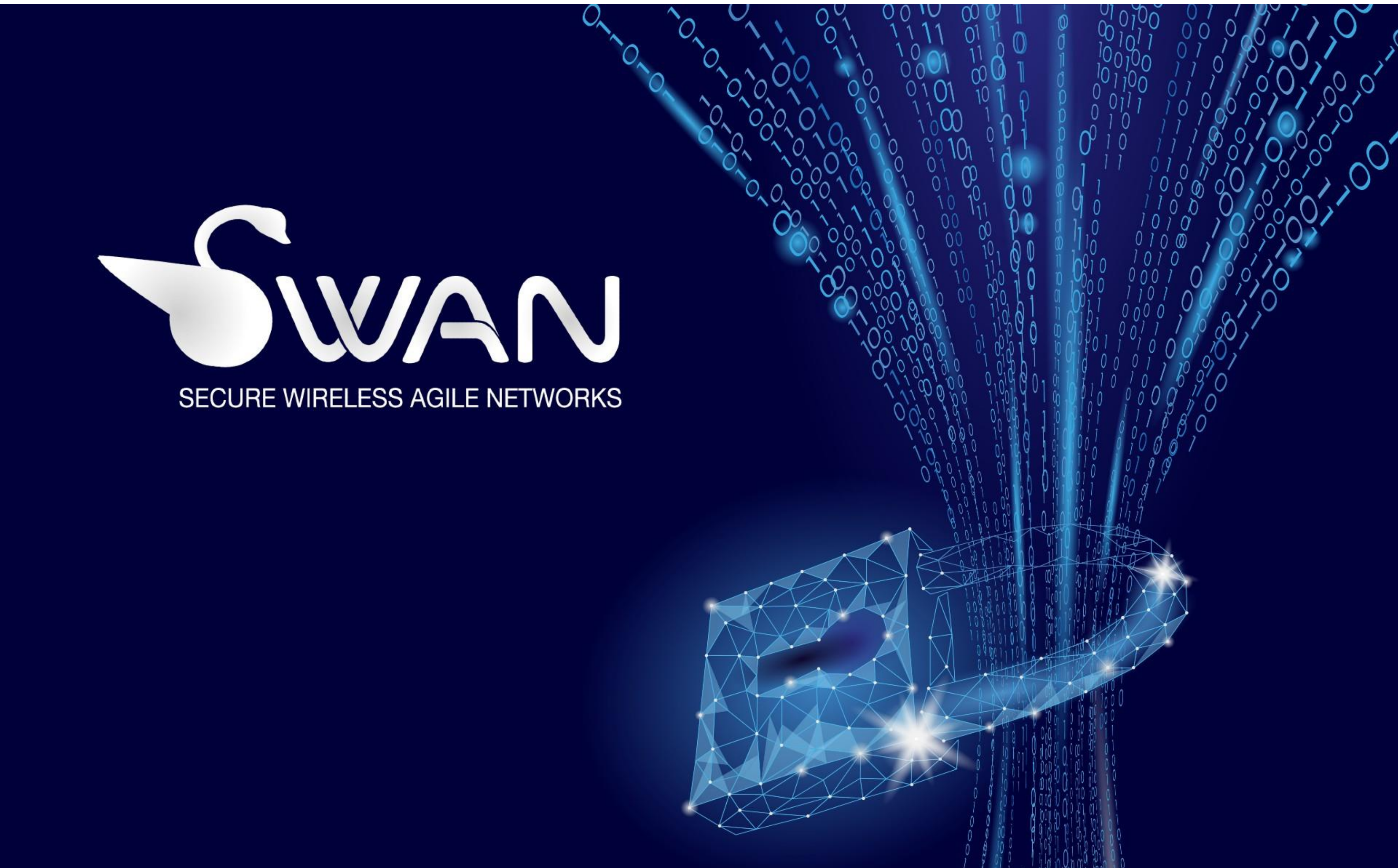


Table of Contents

List of Figures

Executive Summary

Wireless systems are a vital component of modern life and play a key role in how modern society functions, with mobile wireless technology now ubiquitous and the backbone of how we currently communicate both individually and in groups. Wireless connectivity plays a major role in connecting sensors, actuators and control systems together, a part of the internet of things (IoT), with an ever-increasing presence within industry and now the emergence of Smart Cities.

Given the importance of wireless communications to our prosperity and safety, many wireless networks can widely be considered critical national infrastructure with the result security is now an important feature in most wireless systems. Measures such as encryption and authentication have been included in key parts of wireless protocol stacks to facilitate both privacy and resilience. As new threats have emerged, these security measures have necessarily evolved with improvements to counter the potential threat. As a result of this evolution in digital security, wireless communication systems are increasingly hardened to cyber-attack. However, as the threshold to exploitation is increased for an adversary in one area, it is usually the case that attention is then focused on other layers of the system that offer a more vulnerable attack surface.

All radio systems by their nature are vulnerable at the "air interface" level since, by definition and physical laws, this is an open interface. Traditionally, the high cost of the radio transceiver hardware to mount such an attack has been a barrier to this being a widespread problem resulting in it not being widely studied in the technology base that has driven standards development. Low-cost programmable RF and baseband modules are now widely available reducing the entry barrier to an attack at the air interface. Thus, the importance of understanding the vulnerabilities of the "RF Open Attack surface", detecting and mitigating cyber attacks, including the development of resilient transceiver technologies and lower layer protocols. This is remit of the UKRI/EPSRC Secure Wireless Agile Networks (SWAN) Prosperity Partnership described herein, alongside a methodology to assess RF vulnerabilities, example use cases susceptible to RF cyber attacks as well as an overview of SWAN's programme of work.

1. Introduction

In the increasingly inter-connected modern world, communication networks play a pivotal role providing connectivity for people, machines, vehicles, infrastructure, and a wide range of devices (Internet of Things (IoT)). From everyday transactions to health monitoring systems, including the recent Covid 19 test and trace deployment, safe transportation, as well as emerging sensing, monitoring and control in Smart Cities. Increasingly wireless technologies enable these networks directly within a device, or part of the network as well as providing backhaul in cellular networks. However, as radio systems and the Internet become ever more important in society, they become more attractive to elements that wish to profit by subverting them. Cyber sabotage against critical national infrastructure could manifest in a number of ways. Political activists may wish to disrupt public events or cause traffic disruption. Nation state attackers may seek to gain unauthorised access to systems. Disruption to critical infrastructure such as industrial plants, traffic lights, medical equipment, utilities and telecoms could have potentially life- threatening consequences. Financial services will be increasingly reliant on digital automation in the smart city space and will be a key target for cyber attackers.

Cyber attacks aimed at exploiting vulnerabilities in communications networks are commonly directed at the network layer and above [1]. To the wireless interfaces in the network these attacks would be transparent. Attacks of this nature can be mounted remotely, thus there is increasing attention paid to network security in an attempt to close-off this type of attack, for example the more widespread adoption of encryption. However, much less attention has been paid towards attacks mounted at the lower layers of a wireless interface (ie below the network layer) [2]. This type of attack is likely to be mounted at a more geographically localised level (by virtue of the propagation of wireless signals), but in some cases could be mounted remotely if directed at management functions, for example within a wireless network in an attempt to achieve a widespread denial of service in what can be a critical infrastructure, such as a cellular network. In addition to cellular networks, there has been a proliferation of novel wireless technologies over the last 10 years or so addressing the need for long-range low-data rate applications, for example LoRa and SigFox.

All radio systems by their nature are vulnerable at the “air interface” level since, by definition and physical laws this is an open interface. Traditionally, the high cost of the radio transceiver hardware to mount such an attack has been a barrier to this being a widespread problem resulting in it not being widely studied in the technology base that has driven standards development. Low-cost programmable RF and baseband modules are widely available, known as Software Defined Radios (SDR) and this has reduced the entry barrier to attacks at the air interface. Examples include HackRF and NESDR (receive only) family of devices [3]. Further, technical details of the standards are legitimately published on the Internet, and in many cases open-source software is available to provide the basis of an attack system [4].

It is the mission of the UKRI/EPSRC SWAN Prosperity Partnership [5] to conduct research into the security of the wireless interface identifying RF cyber vulnerabilities and types of possible attacks (RF Open Attack Surface depicted in **Figure 1**). SWAN will research detect-and-defence mechanisms against RF cyber-attacks, considering the underlying RF hardware, baseband processing and lower layer protocols of wireless systems and devices. Clearly, the first step is to identify, create and specify attacks that could be mounted against a number of radio systems that are already in widespread use and further adoption is expected to grow significantly in the future. Particular attention will be focused on the range of technologies that are popular and have been increasing market share in recent years, but have not been subject to the rigours of standardisation, as is the case for cellular systems where the 3GPP standardisation body applies. Many of these technologies, including LoRaWAN, started out as long range IoT wireless technologies but, owing to their features and very low cost of ownership, they have become an attractive proposition for systems within critical national infrastructures.

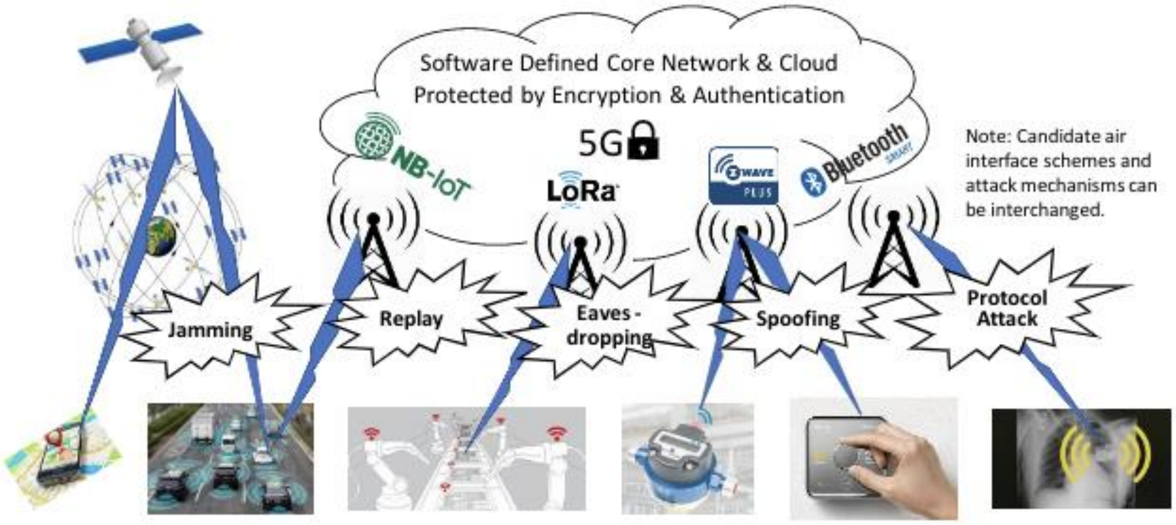

Software Defined Core Network & Cloud
Protected by Encryption & Authentication
NB-IoT
5G
LoRa
Z-WAVE PLUS
Bluetooth SMART
Note: Candidate air interface schemes and attack mechanisms can be interchanged.
Jamming
Replay
Eaves-dropping
Spoofing
Protocol Attack

Figure 1: The RF Open Attack Surface in today's wireless networks

Perhaps the most well-known type of attack directed at the wireless interface is that of jamming, which seeks for example to cause a denial of service. Jamming has in the past been the preserve of electronic warfare leading to the development of anti-jam waveforms and other techniques to mitigate the effects of jamming, and high power jammers have been confined to state actors. Recently there has been the emergence of low and medium power jammers directed at cellular, WiFi and GPS signals that are low cost and available on the internet (either legally or illegally depending on the country in which these are purchased/deployed). Jamming can be a brute force approach by delivering sufficient power into the receiver to cause a loss of service. However, jamming can also exploit parts of the waveform used for control and synchronisation to achieve a more power efficient jammer, and this type of attack can increasingly be mounted using low cost SDR's as mentioned previously.

Another common type of attack involves spoofing where an end device is 'persuaded' to connect to a rogue access point or base station. In this situation traffic can be intercepted from the end user device. Whilst this type of attack has been given consideration in the 3GPP NR standard [6], the 3GPP family of standards maintain backward compatibility to earlier and less secure generations of the standards which can be exploited by the attacker.

The use of wireless devices within Internet of Things (IoT) systems is a current growth market it is also a growth market for cyber attacks on such devices. This is highlighted in **Figure 2**, where the growth in the number of malware packets sent to IoT devices is illustrated and depicts an order of magnitude increase over a five year period. This can be partly attributed to a lower degree of security designed-in in these low cost, lightly regulated systems.

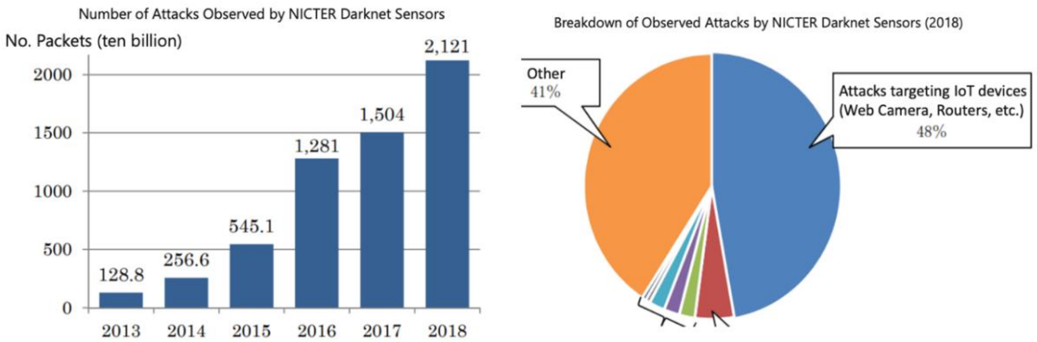


Figure 2: IoT number of attacks from 2013 to 2018 [7]

This white paper explores the types of attack that could be directed at the wireless interface through the application of a threat model, adapted to wireless technologies that has seen wide use within the computer systems community. Specific examples of attacks that have been documented in the literature are given including two case studies covering systems that are commonly subject to attack: the Global Positioning System (GPS) and automotive wireless key entry systems as well as introducing the potential vulnerabilities of Low Power IoT wireless networks.

Finally, the paper outlines the range of topics that the SWAN project will research.

2. A Threat Model for RF Cyber Attacks

There are a number of threat models that have been developed for assessing the threat from attacks in software systems and cyber-physical systems. Threat models are generally divided into two classes: those that catalogue types of threat and those that profile potential attackers in terms of their motivations and methods. Threat models can also be combined to give greater coverage of potential threats. SWAN has adapted the Spoofing, Tampering, Information disclosure, Denial of service, Elevation of privilege (STRIDE) model [8] for wireless communications.

2.1 The STRIDE Model

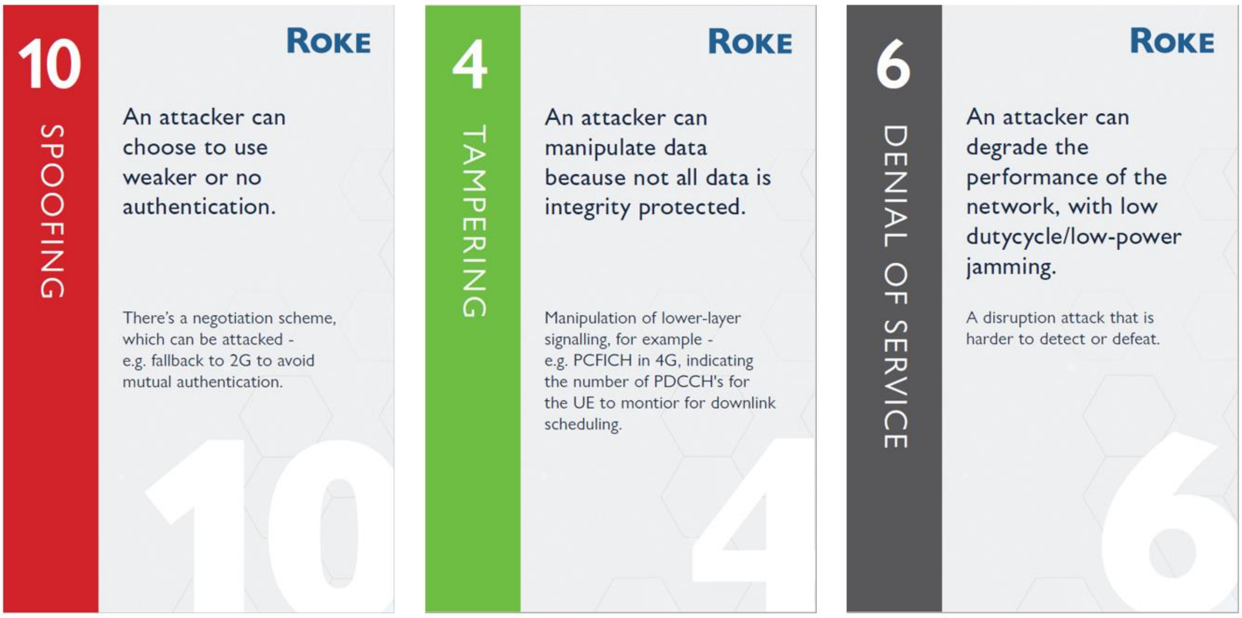
The STRIDE Threat Model was developed in 1999 and was adopted by Microsoft in 2002 [8]. It is the most mature threat model and has been applied to both cyber and cyber-physical systems The STRIDE model, depicted in **Figure 3**, defines a number of generic threats and within each threat a number of possible attacks. It can be applied at the system level or to elements within a system.

	Threat	Property Violated	Threat Definition
S	Spoofing identity	Authentication	Pretending to be something or someone other than yourself
T	Tempering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn’t do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorised to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorisation	Allowing someone to do something they are not authorised to do

Figure 3: STRIDE Threat Categories [9]

The model has become popularised through a set of playing cards that system developers use to ask questions about the security of the system. Although the original motivation was for developing software systems, the threats are generic and can be applied to wireless systems. A set of STRIDE playing cards specific to wireless systems has been produced by the SWAN project partners. Below each of the terms is put into context with respect to wireless systems and examples given of the various types of attack.

Each suit in the deck of cards denotes a threat category, and within each suit a number of possible attacks described. The severity of the attack can be denoted by the playing card number. An example of the cards is shown in **Figure 4** below.


10 SPOOFING ROKE

An attacker can choose to use weaker or no authentication.

There's a negotiation scheme, which can be attacked - e.g. fallback to 2G to avoid mutual authentication.

4 TAMPERING ROKE

An attacker can manipulate data because not all data is integrity protected.

Manipulation of lower-layer signalling, for example - e.g. PCFICH in 4G, indicating the number of PDCCH's for the UE to montior for downlink scheduling.

6 DENIAL OF SERVICE ROKE

An attacker can degrade the performance of the network, with low dutycycle/low-power jamming.

A disruption attack that is harder to detect or defeat.

Figure 4: RF STRIDE Cards

Spoofing: This type of attack refers to a person or a program successfully being identified as part of a wireless network by falsifying data.

Spoofing Examples: In wireless systems, an example could be a base station or access point appearing to be a legitimate device to which a device can connect to. This is a common and easily mounted attack in WiFi where a rogue device appears as a legitimate WiFi access point but is intercepting all traffic routed through the access point. This type of attack is also known as a Man in the Middle attack (MiTM).

In cellular systems ‘standalone base stations’ incorporating a simplified core network implementation can be used to spoof a cellular network. If the standalone base station presents a higher signal strength than the legitimate cellular network, then phones will switch to the standalone base station, and all traffic can be intercepted. A demonstration of this using a standalone Global System for Mobile Communications (GSM) base station was conducted in 2010 [9]. Of the cellular standards, GSM is the most vulnerable to this type of attack as there is readily available open source software for implementing a base station that can run on low end SDR’s. However, the attack can be mounted on 3G and 4G networks, either through implementing a standalone GSM base station, or through forcing phones onto a standalone base station by jamming of the 3G and 4G networks [10].

A common use of spoofing in cellular systems is to capture identity information for example the International Mobile Subscriber Identifier (IMSI). A wide variety of devices, often called IMSI catchers have been developed based around a modified base station [11]. The spoof base station exploits cell selection and cell reselection procedures to obtain identity information from the mobile device and in some cases location of the device. 2G, standards such as GSM are particularly vulnerable [12] as authentication of the handset to the network is only required, however successive generations have, despite security improvements, been shown to be vulnerable to this attack [13].

In a Self-Organised Network (SON), where base stations can self-organise and self-configure, a rogue base station can impact the operation of the network through a variety of mechanisms from falsifying measurement reports to interfering with automatic planning of the Physical Cell Identifier (PCI) resulting in the base station having to re-boot whenever this identifier changes [14].

Tampering: Manipulation or altering of data sent over a wireless link. This could extend not just to information, but also control signalling as part of a denial of service attack. Additionally, software or firmware loaded onto a wireless device could also be altered.

Tampering Examples: By using two WiFi dongles in close proximity and forwarding packets from one dongle to the other (with some driver firmware modifications) it was possible to intercept encrypted packets and thus implement a MiTM [15], whereby user data can be manipulated.

Packet injection is a common attack in WiFi and a form of tampering. Free software is available to mount this type of attack including Airpcap and Aircrack.

Physical tampering of WiFi access points that are not in a secure location is also possible, allowing the attacker to revert the access point to its default settings, as part of an information disclosure attack, for example.

In cellular systems manipulation of the broadcast data content that is read by all User Equipment (UE) on initial access and contains parameters for the UE to determine the configuration of the base station, would result in denial of service. Protocol dissectors available for all cellular standards facilitate this type of attack [16].

Repudiation: Claiming to have executed an action, or failing to act on a command.

Repudiation Examples: In communications protocols, it is common to acknowledge signalling messages. Communication with a rogue wireless device that does not send acknowledgements even though a message is received could be an example of this type of threat. A specific example is where a rogue device intercepts paging messages, and is able to respond faster than the intended recipient, meaning that the state machine in the network transitions to the next state and blocks the later arriving message from the genuine recipient [17].

Information Disclosure: In wireless systems, this is more commonly known as eavesdropping where an interceptor attempts to detect and decode information not intended for them. The most common protection against eavesdropping is the use of encryption.

Information Disclosure Examples: In general, the evolution of cellular standards from GSM through to New Radio (NR) [18] has seen increasing attention paid to interception of traffic. Whilst in GSM encryption was applied to traffic, no encryption was applied to call control signalling. Many vulnerabilities in the A5/1 encryption used in GSM have been exposed dating back to 2003, more recently a method that allowed an interceptor to decrypt data was published on the internet [19]. In the 3G standard Wideband Code Division Multiple Access (WCDMA), a new encryption algorithm was developed, and encryption applied to traffic and control signalling, once the User Equipment (UE) was attached to the network. In the 4G standard further security enhancements were made together with how the network and the UE authenticate each other. In 5G, security has been enhanced further so that all subscriber information is encrypted meaning that no identifiers such as the previous standards International Mobile Subscriber Identity (IMSI) are ever transmitted unencrypted. Vulnerabilities have been identified in the original 5G Authentication and Key Agreement (AKA) protocol [20] and [21]. These vulnerabilities have subsequently been addressed within the 3GPP standards. It should be noted that in all standards, including 5G, no encryption remains an option, set by the infrastructure.

In WiFi, chipsets are available that support a monitor mode, enabling identities like the MAC Address, IP Address and Session ID of any device connecting to an access point with monitor mode to be easily obtained.

Denial of Service: In wireless systems jamming is a denial of service attack. Jamming attacks can take various levels of sophistication from so called barrage jamming to more sophisticated and targeted types of attack exploiting lower layer protocols to deny service.

Denial of Service Examples: Perhaps the simplest form of a denial of service attack is to continuously emit a signal in the desired frequency band causing interference to a legitimate device. This type of attack is often referred to as barrage jamming. There are many unsophisticated jammers openly advertised on the internet that will cover multiple cellular bands and also GPS frequencies. This type of jammer typically emits broadband noise in particular bands, or emits a chirp signal sweeping across particular bands. An example of this type of jammer [22] is shown in **Figure 5** below, which claims a 10W output power across GSM, 3G, LTE, GPS and WiFi bands with claimed effectiveness up to 30m from the device. Jammers with higher transmit powers, having effectiveness over greater areas are also available.

Figure 5: Example Combined Cellular, GPS and WiFi Jammer [22]

This type of jamming can be effective but is inefficient requiring a continuous high transmit power and not exploiting potential vulnerabilities in a particular wireless standard. Other jamming approaches can be more efficient, for example reactive jamming whereby sensing is performed, and on detection of a signal a jamming signal is transmitted. An example of this type of jamming directed at IEEE 802.15.4 (Zigbee) using a low cost SDR is described in [23]. Exploiting particular vulnerabilities in a waveform is a yet more efficient type of attack. An example is taken from LTE where signalling is transmitted in the downlink on a Physical Downlink Control CHannel (PDCCH) that provides the UE with scheduling information, by synchronising to the base station and targeting jamming at the

PDCCH it is then possible to deny service in a more energy efficient manner as the PDCCH only occurs on certain sub-carriers, and symbols within the downlink transmission [24].

Denial of Service attacks on WiFi have been extensively researched. For example, in [15] a number of DoS attacks were implemented using low cost WiFi dongles with open-source driver firmware. This work demonstrated the ability to disable backoff and carrier sense by changing register settings on the device resulting in a device that does not conform to the basic Carrier Sense Multiple Access/Collision Detection (CSMA/CD) protocol used in WiFi resulting in severe reductions in throughput for other devices. Relatively sophisticated attacks on WiFi are made easier by the availability of open-source protocol dissectors for use with tools such as WireShark [25], an example being Airpcap. A common denial of service attack, which can be part of a Spoofing attack is the disassociation or de-authentication attack. Here the attacker sends a de-authentication frame which forces the device off the access point it is currently attached to. This type of attack has been used by hotels in the US and has led to fines being imposed by the FCC, where the hotel forces users off WiFi hotspots onto the hotels (paid for) WiFi [26].

More sophisticated and localised denial of service attacks are possible where the jamming transmitter generates a jamming signal in such a way that this causes signal cancellation at the victim device.

Elevation of Privileges: In computer systems, this attack is concerned with being able to obtain more privileged access such as gaining 'admin rights'. There is a weaker applicability to the lower layers of a wireless communications system, but the ability to load firmware or software onto a device could require such elevated privileges. Malware has been found on smartphone devices [27], within a manufacturer pre-installed app. Also, software updates and GPS data, trusted by the whole system, can constitute 'portals' of 'Elevation of Privilege' attacks.

2.2 STRIDE Threat Analysis

In software systems, the application of STRIDE develops data flow diagrams to identify the different elements of the system and to define its boundaries. In dealing with a wireless system a breakdown into the system elements is possible but that needs to consider the different interactions within the layered structure of communications protocols. In order to achieve a generic breakdown that is applicable across a wide range of wireless systems with differing topologies and characteristics some elements may not be present, or be relatively simple: for example, an antenna system, which in some wireless devices can consist of a single passive element, but can extend to include multiple antenna elements with remote control (as in cellular systems) to fully adaptive antenna arrays. The following generic block diagram of a wireless system is shown in **Figure 6** below. Individual system elements are shown together with interactions between elements for which some protocol is defined with multiple layers. Cross-layer interactions particularly between the Physical Layer, Link Layer and MAC Layer can exist, but are not explicitly shown.

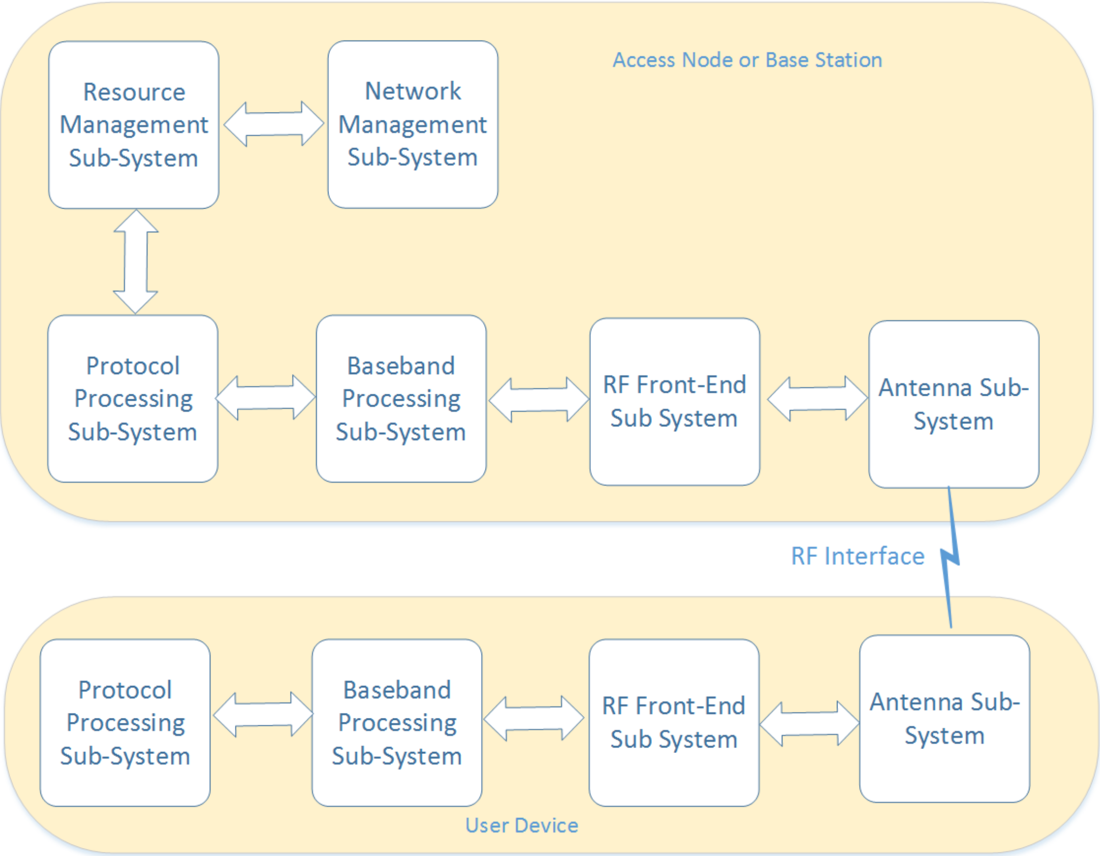

Access Node or Base Station
Resource Management Sub-System
Network Management Sub-System
Protocol Processing Sub-System
Baseband Processing Sub-System
RF Front-End Sub System
Antenna Sub-System
RF Interface
Protocol Processing Sub-System
Baseband Processing Sub-System
RF Front-End Sub System
Antenna Sub-System
User Device

Figure 6: Generic Wireless System for STRIDE Threat Analysis

3. Case Studies

Three examples of RF cyber attacks are outlined below, covering systems not previously covered in section 2, but where such systems are vulnerable to jamming and spoofing, potentially impacting national infrastructure or loss of personal property. The first example is Global Navigation Satellite Systems such as GPS, the second is wireless key fobs widely used in automotive applications, and finally a new class of Low Power Wireless Access Networks (LPWAN) for the wireless interconnection of a multitude of sensors, for example in a Smart City context.

Case Study A - Global Positioning System

Vulnerability of the Global Positioning System (GPS) to jamming and spoofing

The Global Positioning System is a Global Navigation Satellite System (GNSS) [28], providing precise geolocation and time information anywhere in the world, operated by the United States Department of Defence. Many critical services and infrastructure in the UK and around the world depend on GPS and/or other GNSS systems for timing and positioning. Examples of such services include phase synchronisation in power grids (including solar and wind power generation), transaction timings in stock exchanges, airport apron management, traffic control systems, and multi-site synchronisation in cellular networks, as well as location and position tracking data. Despite their importance, GNSS systems are vulnerable to both jamming and spoofing as this was not foreseen as a major issue when GNSS conceived some 50 years ago.

Types of Attack: Jamming and Spoofing

The GPS signal reaches the earth's surface with a spectral power density below the thermal noise floor of the receiver, exploiting processing gain to synchronise and extract navigation messages. The very low received power level makes a GPS receivers extremely vulnerable to jamming from readily available inexpensive devices. There are numerous documented incidents of GPS jamming [29], several of which are outlined below:

The UK SENTINEL project [30] monitored the incidence of GPS jamming at a number of locations during the period October 2012 to December 2013 with some sites detecting up to 10 jamming events per day. Recent studies have indicated that the number of events has increased. There are also a number of documented incidents of aircraft GPS receiver jamming. For example, in August 2016 a Boeing 777-300 lost its GPS guidance prior to landing at Manila's Ninoy Aquino International Airport [31]. Besides jamming, spoofing of GNSS signals is another threat, whereby a localised transmitter generates a replica GPS signal at a higher power level that causes the receiver to report a false position or time. Some spoofing attacks can be easily detected by monitoring the received power level, which could be higher than that expected from a satellite.

In addition to aircraft position manipulation, there are reports from 2017 of numerous vessels in the Black Sea reporting GPS interference, where their on-board receivers were giving their position as inland [32]. Further, when spoofed, some receivers may stop working altogether. Researchers at Carnegie Mellon University simulated a spoofing attack that made the receiver believe that GPS satellites were all at the centre of the Earth [33]. This resulted in a major software failure within the receiver, causing it to stop working.

Multi-GNSS system receivers

Most commercial receivers now receive from multiple GNSS constellations, and this can provide a level of resilience to jamming and spoofing by means of alternative constellation selection. GNSS systems typically transmit in in multiple frequency bands requiring a jammer to spread its power across a greater frequency range. With multiple GNSS constellations being received, any spoofing signal needs to replicate a greater number of satellites making it more difficult for the attacker. However, replicating signals from multiple GNSS constellations is relatively straightforward with current technology [34].

Case Study B - Automotive Security [35]

There are two forms of key car entry systems. With Remote Keyless Entry (RKE) the communications initiation comes from the button activation on the key fob, while for Passive Key Entry and Start (PKES) the initial communications comes from the vehicle. It is the PKES system that is vulnerable to RF Relay Attacks. With PKES, when the key fob is in close proximity to the vehicle (around 1 to 3 m), it will respond to a signal from the vehicle. A valid cryptographic response will then allow entry to the vehicle. When the key fob is not 'in range' the vehicle will always be locked, and it is this range detection that becomes the issue with hacking [36].

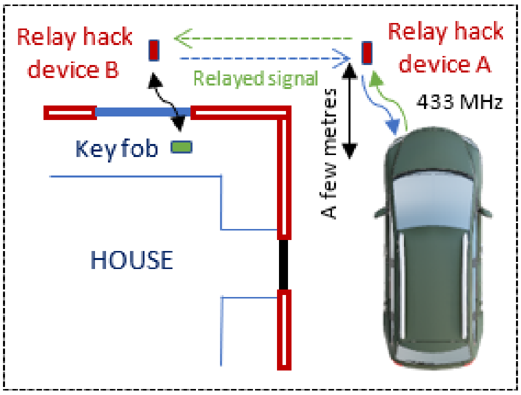


Figure 7: Sequence of Events for a relay attack

With relay hacking, the range can be extended simply by the use of two hacking devices (transceivers) and knowledge of the whereabouts of a 'valid' key fob (probably just located in the house), see **Figure 7.** In this case device A (once in range of the vehicle) will pick up its transmission and then send that to device B that in turn sends to the key fob. This key fob will respond 'correctly' to this transmission and send back the valid cryptographic response to device B that then relays to device A and finally back to the vehicle to gain entry. The 'range' depends on power levels and not on the vehicle to key fob to vehicle communications round trip time, so the signal delay between hacking devices is not detected.

C Low Power Wide Area Networks (LPWAN)

A new class of radio systems has emerged over the past decade aimed at connecting mainly fixed devices such as sensors and controllers to central monitoring and control systems – essentially to connect the "Internet of Things" (IoT). Example applications include:

- Remotely reading utility meters and controlling supply.
- Controlling remote road signs, such as traffic lights.

- Monitoring soil humidity levels at various points in a farmer's field.
- Monitoring mains water flow in a house to raise an alarm if a leak is detected.
- Tracking and managing electric scooter or cycle hire (in conjunction with GNSS tracking).

Such applications have a number of common features: devices communicate short messages with duty cycles ranging from minutes to years, further devices may not be ideally located from an RF point of view, perhaps being placed in a manhole and thus a high propagation loss must be tolerated. Furthermore devices are required to be extremely low power, operating from a battery or powered through energy harvesting with lifespans of up to 15 years.

- Data messages are short and infrequent: utility meter reading < 1 kilobyte once per day; an National Marine Electronics Association (NMEA) Sentence defining a position < 79 characters every few minutes; humidity reading ~10 bytes once per hour; a leak ~100 bytes every few years.
- Radio propagation to remote devices can be very poor. They might be located in a manhole, meter closet, or even buried in damp soil.
- Device power consumption has to be very low. A gas meter must not be mains power connected (for safety) and has to operate for 15 years without battery replacement, and at the end of that time it must still be possible to turn off a valve remotely to isolate the supply. This requirement may of course be traded off with the low data volume and infrequent communications.

Clearly some of these applications are critical, in the sense that safety or economy may threatened if they are compromised.

The obvious way for such systems to communicate is using cellular and many early systems used GSM, often using SMS [37] although GPRS with dedicated SIM cards offered a cheaper alternative. Cellular systems were initially designed for voice connectivity, and later packet data was added. They have shortcomings for such applications: often even the minimum tariff is too high to make the business case viable; the need for regular location updates and the design of the system for quite high mobile transmit power makes it very difficult to achieve very long battery life; and they are not designed for deep coverage such as into manholes or meter closets. Though 3GPP has in recent years recognised the need for alternative cellular systems, a new class of radio system, the LPWAN, has emerged to meet the need.

- Because the cellular industry was not moving to meet the need, such systems tend to be designed to operate in licence-exempt spectrum such as the bands around 868 MHz, where anyone can deploy systems that meet minimum technical requirements. This especially implies quite a low transmit power, limited to 100mW for example.
- The systems have been initially designed by commercial companies to meet a specific requirement and are not "standards" in the regulatory sense. However

the need for widespread support to achieve scale economy has led to proprietary systems being opened up for multiple manufacturers.

- The combination of low permitted transmit power and need for wide coverage (and therefore high link budget) means that LPWAN systems have very narrow information bandwidth. Correspondingly, packet transmission times may be quite long which can create vulnerabilities.
- Ever since GSM was designed the cellular industry has been very concerned about access and information security, so encryption and authentication are baked-in to the standards. The proprietary source of other LPWAN standards, and the fact that they emerged some years ago when cyber security concerns were much lower, means that they may be much less secure.

Examples of LPWAN systems include LoRaWAN and Sigfox. LoRA [38] was initially developed by Semtech Corporation (USA) in an RF chipset to implement the transceiver and protocol engine. It is now supported by a number of companies in the LoRa Alliance [39] making chipsets and other equipment and systems. LoRaWAN is a definition of network and end-to-end protocols by which Gateways (i.e. base stations) can be connected to a back-end infrastructure, and data exchanged between “Nodes” (i.e. devices) and central servers. The specification provides for 2-way communication (including message acknowledgement and transmission to the end device) and uses AES128 for end-to-end encryption. The LoRa air interface uses chirp spread spectrum to provide some immunity against interference. LoRa is in principle band-agnostic but in the UK for example has been deployed in the 868 MHz band.

Sigfox [40] is a very simple uplink narrow band system designed for basic data collection, however bi-directional communications has recently been added. It has been used for example for smoke and fire alarms; and residential leak detection. It has minimal data protection both against errors and subversion. The lack of an effective downlink makes it unsuitable for serious applications since the sending node cannot have confidence that an urgent message (a fire or a leak for example) has been registered. In the UK it has also been deployed in the 868 MHz band. Note that the inability to update security credentials over the air in a Sigfox node is a cybersecurity shortcoming.

Note that the 868 MHz band is also used by other systems and devices such as Zigbee which in parts of the UK provides the “home area network” used in smart meter installations.

LoRaWAN is being widely deployed round the world for a number of IoT applications, and so the security of the system is of concern. A number of studies have been published into LoRaWAN cybersecurity and susceptibility to jamming [41] [42] [43] and it is clear that the system can be subverted. Also, COTS (commercial off-the shelf) hardware for both gateways and nodes, including chipsets; and software; are readily available, and their communication credentials readily accessible. Another aspect is that the system can operate at very low signal levels, an advantage for system coverage but resulting in only low powers being needed for jamming. A specific jamming attack on LoRaWAN is described in Aras et al [41]. The authors describe *inter-alia* a “wormhole attack” which could be mounted as follows.

- We assume that a public LoRa gateway is set up to serve an area and is used to monitor security alarms. A raid is planned on a warehouse in the area, which has a LoRa Node connected to the security alarm communicating with the alarm management company.
- The gang involved sets up a LoRa jamming node made using COTS hardware close to the Gateway with a fast communication link (using for example LTE modems) (the "wormhole") to another node close to the target premises that is capable of receiving LoRa transmissions from the security system node; with some simple local packet processing (that the above reference shows is well within the capability of for example a Raspberry Pi).
- When the security alarm sends a message on detecting an intrusion, it sends a trigger to the jamming node through the wormhole that enables it to transmit a jamming signal to block the Gateway from receiving the specific signal from the alarm.

This attack is possible because off the shelf LoRa hardware is available, details of the system are in the public domain; and LoRa on-air messages are rather long so the jamming node can react quickly before most of the message has been received at the gateway. The jamming system only needs to be activated for the duration of the raid. From the system point of view, since only a small number of packets from one Node will be corrupted the jamming may not be noticed at all.

Given its deployment for critical applications ways to detect and mitigate attacks need to be understood. The operational aspects of LoRaWAN attacks seem to have been less researched, in other words how would an attacker:

- Know that LoRaWAN is being used for a particular application in a given geographic area?
- Identify the locations of Gateways and Nodes of interest?
- Practically, determine the optimum type of attack on the system and locations from which to jam and/or intrude on the system?

Understanding these aspects should illuminate investigation of possible jamming techniques and help to specify mitigation measures.

For mitigating against attacks there are further issues:

- What level of system monitoring information is available from both Gateways and Nodes that might be processed to indicate jamming or intrusion?
- How might such information be gathered from Nodes if they have been compromised?
- Since the object of deploying a LoRa network is wide area coverage at low cost, how can additional system monitoring stations be deployed to detect malicious transmissions without too much impact on economics?

- Given that systems such as Zigbee are also deployed in similar spectrum and probably in overlapping areas, would LoRaWAN jamming affect Zigbee and could the Zigbee infrastructure be used to provide additional information?

These are potentially important areas for research that will be explored by SWAN (see section 5).

4. RF Cyber Research Challenges

Wireless connectivity is a key societal enabler, and any disruption can have significant consequences [44], thus there is an imminent need to engineer secure, resilient, agile and sustainable wireless technology for future communications systems. Building-on the RF threat model described in section 2 and the following use cases, the following research challenges (RC) can be defined and from which a research programme has evolved as outlined in section 5:

RC1: Threat Synthesis and Assessment:

Understanding the vulnerabilities of wireless to RF cyber attacks, efficacy of attack mechanisms and impact upon end users.

RC2: RF Cyber Detection & Defence:
Power efficient, fast, and low-cost detection schemes alongside countermeasures.

RC3: Cyber Secure Radio Design:
Resilient and agile RF transceivers making SDR a reality as well as opening up new mechanisms for spectrum management and use.

RC4: Secure Dynamic Spectrum Access:
Application of RC3 alongside secure and robust sharing protocols to evolve the widespread adoption of Spectrum Sharing in future networks, such that more spectrum becomes available for evolving applications and needs.

5. Secure Wireless Agile Networks (SWAN)

The UKRI/EPSRC Prosperity Partnership SWAN is addressing the 4 research challenges outlined above through an industrial and academic 5-year programme of research, with the following objectives:

1. Establish a methodology to understand and synthesize attacks on communications systems vectored through the radio interface;
2. Develop methods for effective and efficient RF threat detection, analysis and mitigation;
3. Develop methods to design and implement agile and resilient transceivers;
4. Develop a testing methodology and resource for radio networks to evaluate threats and mitigations, avoiding the tendency to "group-think" that could exclude various types of attack or defence;
5. Apply SWAN's secure agile and robust RF technology to Dynamic Spectrum Access to enhance spectrum utilisation whilst mitigating misuse.

Key features of the SWAN's research include:

- Leveraging of spatial domain signal suspension to counteract non-system interference/ jamming as many air interface standards now mandate multi-antenna technologies (MIMO). Significant opportunities exist to exploit the common needs of wireless connectivity and RF cyber protection.
- RF circuit topologies offering greater frequency agility against jamming (blocker resilience) as well as facilitating truly Dynamic Spectrum Access as a means of future spectrum management will release previously unused geographical spectrum locations.
- Application of Artificial Intelligence (AI) and Machine Learning (ML) techniques to control the use of channels to increase capacity and mitigate against RF Cyber attacks potentially offers efficient and robust solutions.
- Fast and accurate identification of legitimate and illegitimate users via spectrum monitoring is a key enabler for resilient wireless access. Here, exploiting the presence of multiple distributed sensors (antennas) and the application of ML/AI to enable detection of less obvious attacks, or robust non-system interference detection based on orthogonal sub-space projection in detecting jamming/ interference events will stimulate new solutions.

In order to facilitate a greater understanding of RF Cyber attacks and benchmark SWAN's technology offerings, penetration testing (pen-test) will underpin the validation and associated performance optimisation. LoRa has been selected as the first candidate air interface to pen-test. Here, using conductive testing, waveform monitoring and penetration injection testing of a variety of jamming and spoofing techniques is underway. This facility will be expanded to include other candidate air interfaces, such as NB-IoT, as well as assess the performance of SWAN's RF front-end technology developments.

References

[1] A. Rashid et al (Editors), “The Cyber Security Body of Knowledge”, Oct 2019, [Online] https://www.cybok.org/media/downloads/cybok_version_1.0.pdf

[2] D. Lund, “Wireless Communications Cyber Security,” *IET Engineering & Technology*, March 2017, doi 10.1049/etr.2015.0118

[3] Bliley Technologies, “10 Popular Software Defined Radios (SDRs) of 2021,” Feb 2020, [Online] https://www.cybok.org/media/downloads/cybok_version_1.0.pdfhttps://blog.bliley.com/10-popular-software-defined-radios-sdr

[4] CC Labs, “RFCrack - A Software Defined Radio Attack Tool,” Mar 2020, [Online] https://github.com/cclabsInc/RFCrack

[5] Secure Wireless Agile Networks (SWAN), [Online] https://www.swan-partnership.ac.uk/

[6] 3GPP, “5G; Security architecture and procedures for 5G System,” Oct 2018, [Online] https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf

[7] Y. O. Hikohiro, Y Lin, “Understanding the IoT threat landscape and a home appliance manufacturer's approach to counter threats to IoT”, Dec 2019, [Online] https://i.blackhat.com/eu-19/Thursday/eu-19-Lin-Understanding-The-IoT-Threat-Landscape-And-A-Home-Appliance-Manufactures-Approach-To-Counter-Threats-To-IoT-2.pdf

[8] Microsoft, “The STRIDE Threat Model,” Dec 2009, [Online] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[9] N. Shevchenko, “Threat Modelling: 12 Available Methods,” Dec 2018, [Online] https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

[10] R. Krenz & S. Brahma “Jamming LTE Signals,” Aug 2015, IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), DOI:10.1109/BlackSeaCom.2015.7185089

[11] D. Goodin, “Low-cost IMSI catcher for 4G/LTE networks tracks phones’ precise locations,” Oct 2015, [Online] https://arstechnica.com/information-technology/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/

[12] G. Cattaneo et al, “Security Issues and Attacked on the GSM Standard: A Review”, *Journal of Universal Computer Science*, vol. 19, no. 16, 2013

[13] Roger Piqueras Jover, “LTE protocol exploits – IMSI catchers, blocking devices and location leaks", https://www.slideshare.net/EC-Council/lte-protocol-exploits-imsi-catchers-blocking-devices-and-location-leaks-roger-piqueras-jover , accessed 20/04/2021

[14] A. Shaik, R. Borgaonkar, "LTE Network Automation under Threat", [Online] https://i.blackhat.com/us-18/Wed-August-8/us-18-Shaik-LTE-Network-Automation-Under-Threat-wp.pdf

[15] M. Vanhoef, F. Piessens, "Advanced Wi-Fi Attacks using Commodity Hardware", *Proceedings of the 30th Annual Computer Security Conference*, 2014.

[16] P. Quantin, "Medium Access Control (MAC) for LTE," Nov 2011, [Online] https://wiki.wireshark.org/MAC-LTE

[17] Nico Golde et al, "Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks", https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_golde.pdf , accessed 20/04/2021

[18] 5G Networks, "5G NR: New Radio," Aug 2019, [Online] https://www.5g-networks.net/5g-technology/5g-nr-new-radio/

[19] C. Paget, "GSM: SRSLY?", *26th Chaos Communications Conference*, 2009. [Online]. Available: https://fahrplan.events.ccc.de/congress/2009/Fahrplan/events/3654.en.html

[20] D. Basin et. al., "A Formal Analysis of 5G Authentication*", Proceedings of the 2018 ACM SIGSAC Conference on Computer Communications and Security*, pp. 1383-1396, January 2018.

[21] C. Cremers, M. Dehnel-Wild, "Component Based Security Analysis of 5G Channel Assumptions and Session Confusion", *Network and Distributed Systems Security Symposium (NDSS)*, 2019.

[22] www.jammer-store.com [Online]

[23] M. Wilhelm, I. Martinovic, J.B. Schmidt, V. Lenders, "Reactive Jamming in Wireless Networks- How Realistic is the Threat?", *Proceedings of the 4th ACM Conference on Wireless*

[24] M. Lichtman et. al., "LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation," *IEEE Communications Magazine,* pp 54-61, April 2016.

[25] https://www.wireshark.org/ [Online]

[26] K. Hetter, "Marriott fined $600,000 by FCC for Blocking Guests' Wi-Fi", *CNN*, 2014. [Online] https://edition.cnn.com/2014/10/03/travel/marriott-fcc-wi-fi-fine/index.html

[27] Cyber News, "TCL Weather Malware Found Pre-Installed on Alcatel Phones", https://sensorstechforum.com/tcl-weather-malware-pre-installed-alcatel/#:~:text=A%20new%20security%20report%20shows%20that%20Alcatel%20smartphones,available%20on%20the%20Google%20Play%20Repository%20as%20well , accessed 20/04/2021

[28] European GSA, "What is GNSS?", Nov 2019, [Online] https://www.gsa.europa.eu/european-gnss/what-gnss

[29] Blackett Review, "Satellite-derived time and position: a study of critical dependencies," Jan 2018, [Online] https://www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review

[30] C. Curry, “SENTINEL Project Report on GNSS Vulnerabilities”, *Chronos Technology*, April 2014

[31] P. Tullis, “GPS Is Easy to Hack, and the U.S. Has No Backup,” Dec 2019, [Online] https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup

[32] Hambling D ‘Ships fooled in GPS spoofing attack suggest Russian cyberweapon’ New Scientist, 2017, [Online] www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon

[33] Nighswander T and others ‘GPS software attacks’ *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 450-461

[34] G. Buesnel, “With GNSS Spoofing Attacks on the Rise, Resilience and Robustness Go Hand-in-Hand,” Sept 2020, [Online] https://galileognss.eu/with-gnss-spoofing-attacks-on-the-rise-resilience-and-robustness-go-hand-in-hand/

[35] C. Evans, “Keyless car theft: What is a relay attack, how can you prevent it, and will your car insurance cover it?”, April 2020, [Online] https://leasing.com/car-leasing-news/relay-car-theft-what-is-it-and-how-can-you-avoid-it/

[36] F. D. Garcia et al, Lock It and Still Lose It —on the (In)Security of Automotive Remote Key-less Entry Systems, *25th USENIX Security Symposium*, Aug 2016

[37] S. Amudha & N. Snehalatha, 2016, “SMS Controlled Smart Home System In IOT,” International Journal of MC Square Scientific Research, 8. 1-8, 10.20894/IJMSR.117.008.001.001.

[38] https://www.semtech.com/lora [Online]

[39] https://lora-alliance.org/ [Online]

[40] https://www.sigfox.com/en/what-sigfox/technology [Online]

[41] E. Aras, N. Small, G. S. Ramachandran, D. Stéphane, W. Joosen, D. Hughes, (2018), “Selective Jamming of LoRaWAN using Commodity Hardware,” *MobiQuitous 2017*, Melbourne, VIC, Australia, November 7–10, 2017, pp. 363–372, https://doi.org/10.1145/3144457.3144478

[42] M. Ingham, J. Marchang, D. Bhowmik, (2020), “IoT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN”, *IET Information Security*, 14 (4), pp. 368-379, https://doi.org/10.1049/iet-ifs.2019.0447

[43] Trend Micro, (2021), “The Current State of LoRaWAN Security: Technical Brief,” [Online] https://documents.trendmicro.com/assets/pdf/The%20Current%20State%20of%20LoRaWAN%20Security.pdf

[44] www.cpni.gov.uk/cyber [Online]