Protection of Mobile and Wireless Networks Against Service Availability Attacks

by

Ginés Escudero Andreu

Supervisors:

Dr. Konstantinos Kyriakopoulos, Dr. James Flint

and Prof. David Parish

The Wolfson School of Mechanical, Electrical and Manufacturing Engineering

Loughborough University

Doctoral Thesis

Submitted in partial fulfillment of the requirements

for the award of

Doctor of Philosophy

of Loughborough University

Submitted on the 31st July 2017

«...para Lola, Ginés y María,
por ser siempre luz en mi camino...»

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements.

Ginés Escudero Andreu
Submitted on the 31st July 2017

Acknowledgements

Firstly, I would like to express my special appreciation and sincere gratitude to my recently retired supervisor *Prof. David J. Parish*, for the continuous support and valuable guidance. His advice and encouragement contributed positively to give shape to this research project, and helped directing my research experiments towards the acquisition of successful results.

A special thanks to my friend, last-year supervisor and always research mentor *Dr. Konstantinos Kyriakopoulos*. I can certainly say that this thesis would not be possible without your constant encouragement, strong support and relentless effort to keep my motivation high, correcting my research direction when I felt lost and endlessly praising of my potential to give me the courage when I needed the most.

I would also like to mention *Prof. Raphael C.-W. Phan* for believing in me for this research project, persuading me to apply for a scholarship and guiding me all along the first year. I feel specially grateful to *Dr. James Flint*, for being brave enough to take the supervisor role when I was reaching the end of the writing-up year, and guiding me to the completion of this thesis with bravery and admirable empathy with my personal circumstances.

I have no words to express how grateful I am to my parents *Gines Escudero* and *Lola Andreu*, my sister *María Escudero* and rest of my wonderful family, for not giving up on me and walking next to me through all this long journey. I certainly believe that this thesis would not exist without your relentless support when I had no breath, your wise advice when I was full of doubts, the constant motivation on each of our conversations, and the huge amounts of love and caring proffered. I feel so proud and extremely lucky of having you all on my life.

This thesis has been positively influenced by all my colleagues from the High-Speed Network (HSN) research group at Loughborough University: *Abdulrazaq Almutairi*, *Francisco Aparicio*, *William Johnson*, *Rui Li* and *Segun Aina*. Your insightful guidance during our daily discussions has been a source of knowledge for me, and a huge contribution to my work. I could not have even dreamt of having a better research group, and truly thank you all for not giving me a chance to doubt about my potential.

My sincere thanks also goes to all the people I met while conducting my research, who ended up composing my little family in the UK. I would not be fair if I were not showing my gratitude to *Anna Sammarco*, *Bea Fernández*, *Carlos Castelló*, *Celia Incerti*, *Isabelle Renninger*, *Mario Carandente*, *Nuria Lastra*, *Paula Cosar*, *Tony Lafuente* and *Vanessa Silvestre*. Thank you for sharing with me what have already become some of the best moments of my life. You are the reason why I still can boast of keeping my mental health after going through the tough times of this Ph.D.

A special mention of appreciation for Maria Lima, who joined me on this endeavour towards the end of the journey. She helped me find the energy required to complete the writing up phase and taught me how important smiling is, no matter how hard the past.

Last but not least, I do also want to express my gratitude to *Prof. Michele Vadursi* and *Dr. Diego Santoro* for their collaboration on this research project, the staff at the old *School of Electronic, Electrical and Systems Engineering* (and the new re-branded School of Mechanical, Electrical and Manufacturing Engineering) and *Loughborough University* for funding this project and making it possible.

Abstract

Cellular and wireless communications are widely used as preferred technology for accessing network services due to their flexibility and cost-effective deployment. 4G (4th Generation) networks have been gradually substituting legacy systems, relying on the existing commercial and private Wireless Local Area Network (WLAN) infrastructures, mainly based on the IEEE 802.11 standard, to provide mobile data offloading and reduce congestion on the valuable limited spectrum. Such predominant position on the market makes cellular and wireless communications a profitable target for malicious users and hackers, justifying the constant effort on protecting them from existing and future security threats.

Radio communications are exposed to the most basic Denial-of-Service (DoS) attack known as radio jamming, aiming at disrupting the communications by tackling the physical layer, or the more complex intelligent jamming, exploiting vulnerabilities on specific communication protocols to disrupt the service. Jamming attacks have been widely studied, being possible to reduce or completely counteract their impact on the network. Conversely, intelligent jamming attacks are easily misclassified as legitimate activity due to its complex detection, offering a powerful solution for malicious users to launch selective attacks against specific target nodes.

The work conducted on this thesis has proven effective for strengthening both, 4G and Wireless Fidelity (Wi-Fi) networks, by implementing a new detection mechanism to detect DoS attacks in real time. The proposed mechanism provides an efficient and lightweight Intrusion Detection System (IDS) for identifying intelligent jamming attacks against service availability.

The initial experiments tackle first a virtual jamming attack exploiting the CSMA/CA mechanism on IEEE 802.11 networks, which has been reproduced and successfully detected on a test-bed with real-life scenarios. The proposed metrics monitor the difference on the Network Allocation Vector (NAV) value, the frame inter-arrival time (or DeltaTime), the difference on the Frame Sequence Number (FSN), the data Throughput (T) and the Frame Check Sequence (FCS) error rate.

The detection performance provides a 100% DR when using the NAV metric individually, only reduced to 88.93% and 66.67% when combined with the DeltaTime and CRC metrics

respectively. The T metric has proven more effective when the nodes are located far from the AP, while the DeltaTime obtains better results on the analysis of TCP traffic.

Additionally, three metrics are suggested for detecting an intelligent jamming attack on the Radio Resource Control (RRC) layer of the Long Term Evolution (LTE) standard. This attack exploits the plain-text transmission of the International Mobile Subscriber Identity (IMSI) to perform a DoS attack against the core network. The main proposed LTE metric, Connection Request Rate (CRR), provides an overall 98% DR, obtaining its best performance when combined with the Success Rate (SR) metric to achieve a 100% DR. The last metric, Session Mean Time (SMT), registers DR values above 93% in 2 out of 3 scenarios, confirming its suitable to detect the attack.

The proposed mechanism applies Dempster-Shafer theory of evidence as data fusion technique to reveal anomalies, combining the evidences collected from the metrics. Complimentary, a Basic Probability Assignment (BPA) function is computed for performing live evaluation of each metric and classifying the data frames as malicious, normal or uncertain cases.

This thesis introduces a test-bed designed to evaluate virtual jamming attacks in Wi-Fi networks, and describes the use of a LTE emulator for replicating the studied DoS attack. Results are collected for both technologies and analysed with the proposed algorithm to assess its detection performance. Finally, conclusions are extracted from the analysis, proposing further improvements and research directions for strengthening future cellular and wireless communication systems.

Table of contents

List of figures

List of tables

Nomenclature

Acronyms / Abbreviations

3GPP 3th Generation Partnership Project

4G 4th Generation of mobile communications

ACK Acknowledgement

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AP Access Point

AS Access-Stratum

AV Authentication Vector

BPA Basic Probability Assignment

BSSID Basic Service Set Identifier

CPU Central Processing Unit

CRC Cyclic Redundancy Check

CRR *Connection Release Rate* metric for LTE

CSMA/CA Carrier-Sense Multiple Access with Collision Avoidance

CTS Clear-To-Send

CW Contention Window

DCF Distributed Coordination Function

DIFS DCF Inter-frame Space

DL Data Link layer

DoS Denial-of-Service

DR Detection Rate

D − S Dempster-Shafer

eNB evolved-Node B

EPC Evolved Packet Core

EPS Evolved Packet System

ESMCP Emergency Services Mobile Communications Programme

ESN Emergency Services Network

E − UTRAN Evolved Universal Terrestrial Radio Access Network

FCS Frame Check Sequence

FIFO First-In/First-Out

FN False Negative

FNR False Negative Rate

FP False Positive

FPR False Positive Rate

FSN Frame Sequence Number

GSA Global mobile Suppliers Association

GSM Global System for Mobile communications

GUTI Globally Unique Temporary Identity

HSS Home Subscriber Server

IDS Intrusion Detection System

IEEE Institute of Electrical and Electronics Engineers

IMSI International Mobile Subscriber Identity

IoT Internet-of-Things

IP Internet Protocol

ISP Internet Service Provider

IV Initialization Vector

LLC Logical Link Control layer

LTE Long Term Evolution

MAC Medium Access Control

ME Mobile Equipment

MitM Man-in-the-Middle attack

MME Mobile Management Entity

MNO Mobile Network Operator

NAS Non-Access-Stratum

NAV Network Allocation Vector

OSI Open Systems Interconnection

OSR Overall Successful Rate

PCAP Packet Capture

PDCP Packet Data Convergence Protocol

PHY Physical layer

PPV Positive Predictive Value

QoS Quality-of-Service

RADIUS Remote Authentication Dial-In User Service

RAN Radio-Access Network

RAT Radio-Access Technology

RLC Radio Link Control

RRC Radio Resource Control

RTS Request-To-Send

SIFS Short Inter-frame Space

SME Small and Medium Enterprise

SMT *Session Mean Time* metric for LTE

SR *Success Rate* metric for LTE

SW Sliding Window

TCP Transmission Control Protocol

TKIP Temporal Key Integrity Protocol

TN True Negative

TNR True Negative Rate

TP True Positive

TPR True Positive Rate

UE User Equipment

UMTS Universal Mobile Telecommunications System

USIM Universal Subscriber Identity Module

WAN Wide Area Network

WEP Wired Equivalent Privacy

Wi−Fi Wireless Fidelity

WiMAX Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Networks

WNIC Wireless Network Interface Card

WPA Wifi Protected Access

WSN Wireless Sensor Networks

CHAPTER 1

Introduction

Wireless communications are widely used globally and heavily integrated in our life, offering an affordable and easy access to network services without demanding neither a complex infrastructure nor expensive equipment to be deployed. The combination of a secure and reliable infrastructure to procure Intranet and Internet services, together with the flexibility of having a non-physical endpoint link and seamless connectivity when in motion, makes this technology equally appealing for enterprise and consumer solutions.

In a similar manner, mobile communications provide a wider coverage while still offering the same advantages and minimal differences when the actual user data throughputs are compared. *Long Term Evolution Advanced* (LTE-Advanced) cellular networks have a maximum peak data rate on release 10 of 1.5 Gbps and 3Gbps for uplink and downlink [1] respectively, against the 7.2 Gbps peak data rates of the latest IEEE 802.11ad standard [2] currently available in the market. Further releases are aiming at reducing this gap and providing faster data rates to cope with the constant increase of mobile subscribers, and the exponential growth [3] of user data consumption.

Although the deployment cost is much higher if cellular and *Wireless Fidelity* (Wi-Fi) networks are compared, the current figures of active subscribers, and future forecast, make the investment very profitable and attractive for *Mobile Network Operators* (MNOs). The latest survey produced by Ericsson estimates the use of mobile broadband services in more than 7.5 billions subscribers worldwide for 2016, forecasting an increase to 9 billions by the end of 2022 [3].

The actual perception of current society trends reveals a prominent future for non-wired technologies, where the *Internet-of-Things* (IoT) revolution is actively contributing to increase the number of devices connected to the Internet [4] and the expansion of *Wireless Sensor*

Networks (WSNs). Furthermore, young generations become users of multiple mobile gadgets since the very beginning of their life, adding more challenges for the MNOs and *Internet Service Providers* (ISPs) to cover new user needs and quickly adapt to the required increase of access bandwidth, to cope with the data-traffic demand.

Looking at market analysis reports, the perception is easily acknowledged, identifying a changing pattern in the way users are consuming data services [5], with a dominant position of wireless and cellular technologies over the conventional wired Ethernet infrastructures. Furthermore, the estimated forecast predicts a massive fall on traffic coming from fixed network access from 52% in 2015 to 33% by 2020, forcing a rapid evolution of the technology to cope with the constantly-increasing number of active nodes and the volume of data to be processed by cellular and wireless technologies.

This phenomenon can also be explained by looking at the increase on the use of WiFi networks as principal technology for cellular traffic offloading, registering a 63% of the traffic offloaded from 4^{th} *Generation of mobile communications* (4G) networks in 2016 [5]. Furthermore, the traditional model of complex and expensive deployment of IT infrastructures in corporate networks is being gradually replaced to facilitate the creation of flexible workspaces. Using open-space offices with hot-desks facilitates co-working in collaborative environments, with a 22.9% increase in conversion from traditional office services to co-working spaces [6] in 2016. This office model relies on IEEE 802.11 as the predominant technology for delivering on-premises and cloud-based business network services with a minimal investment and easy adaptability to the constant redistribution of workspaces across the office.

1.1 Security communication systems

Every communication system should be designed taking security into account, focusing on six main pillar or principles [7]: integrity, availability, confidentiality, authentication, authorization and non-repudiation. Multiple solutions have been developed over the years since early releases of wireless and cellular communication standards, aiming at providing mechanisms to protect each of these principles.

Protecting the communication channel is usually achieved using encryption algorithms to preserve confidentiality, adding hash functions or *Cyclic Redundancy Check* (CRC) codes as integrity check of the information transmitted. The authentication and authorisation is usually grouped into the user account management system, requiring the exchange of a secret parameter only known by sender and receiver, such as a password or public/private key pair.

However, it is common to incorrectly associate availability with maintaining the communication system running, ignoring allthe range of threats a system should be protected from

to guarantee a reliable service. These actions are beyond the correct dimensioning of the network, to cope with current demand and the expected growth. Active security mechanisms, such *Intrusion Detection Systems* (IDS), are essential for protecting the system against service disruptions due to bad-intentioned users.

Unfortunately, communication systems constantly evolve at the same speed as the number of security threats they are exposed to, exploiting vulnerabilities and weaknesses to compromise them. Despite of the massive effort taken by the research community, standardisation bodies, manufacturers and security companies for enhancing wireless and cellular communications, new threats arise every year, requiring amendments on the technology specifications. The proliferation of global cyber-attacks, including hacktivism and cyber-crime, together with a constant coverage of new threats and security breaches by the media, have raised awareness of how relevant security is for digital communications and the requirement of additional efforts to strengthening our communication systems.

Since the inception of the IEEE 802.11 standard[8] back in 1997, security has always been a major concern due to the natural openness of the radio channel and the inexpensive equipment available in the market for intercepting and/or disrupting the communications. As several papers[9–12] revealed, the number of identified vulnerabilities ranges from basic network traffic analysis and eavesdropping, due to the openness of the communication channel, up to more complex active attacks, where the attacker intentionally performs radio emissions to conduct the attack.

Looking at the cited list of active attacks, it is possible to include the aforementioned *Denial-of-Service* (DoS) attacks, aiming at disrupting the availability of the communication service; Masquerade attacks, where the attacker impersonates the identity of a legitimate user; or Replay attacks, where the malicious user can take advantage of the information extracted during the monitoring period to gain legitimate access to the systems impersonating a legitimate node, or even disrupt the communications for a particular node by constantly replaying disassociation messages previously captured.

LTE networks have been suffering similar threats, as reported within the research community since early releases of the standard. Initial attacks were able to disclose the *International Mobile Subscriber Identity* (IMSI) value of legitimate subscribers by passively listening to the channel [13, 14], or even gaining access to IP network parameters after tampering a femtocell device [15]. Multiple solutions have been published aiming at strengthening the *Authentication and Key Agreement mechanism* (AKA), which is the main vulnerability exploited in most of the documented attacks. However, no action has been taken by the standardisation body to mitigate it.

This thesis is focused on the definition of new security mechanisms for wireless and 4G cellular networks, with the aim of providing safer services to the end-user and resilience on the MNO's core network. In particular, the approach presented on this thesis focus the interest on DoS attacks tackling both technologies, imposing an important threat for critical services such as first responders, military networks and public services using Wi-Fi and LTE as main technology for *Wireless Local Area Networks* (WLAN) and *Wide Area Network* (WAN) services, respectively. A mandatory zero tolerance policy must be applied when assessing the infrastructure against potential service disruptions, system failures and QoS standards for public communication services [16].

1.2 Service availability in radio communications

Service availability for wireless and cellular communication system is crucial, preventing MNOs and corporations from suffering important loses whenever an outage occurs in their networks due to customer claims and expensive fines imposed by public regulatory entities. The harmful effects of a service disruption become more obvious when considering the gradual replacement of legacy communication systems for public services with LTE technology [16–19].

The UK is about to initiate the testing phase of the next *Emergency Services Network* (ESN), as part of the *Emergency Services Mobile Communications Programme* (ESMCP) [20], based on LTE technology. Public services, including emergency units of fire-fighters, police and first responders, will relay on an LTE network where any service disruption could cost hundreds of lives. IEEE 802.11 technology has also been used as quick and cheap deployment technology for fast response in natural catastrophes such as the Indian Ocean or Haiti tsunamies [21, 22], in combination with other WANs technologies such as *Worldwide Interoperability for Microwave Access* (WiMAX).

MNOs are aware of how crucial service availability is for their customers, having a negative impact on their life whenever an unexpected service disruption occurs. Moreover, the legislation and regulatory entities protect service availability with strict compliance regulation [23], affecting every telecommunication provider. In addition, they are obliged to meet conditions agreed on the contract and Service-Level Agreement (SLA) when a customer acquires their services. Failing to do that could result in facing the risk of economic penalties, customer compensation for the downtime period and, most importantly, invaluable damage to their brand reputation due to the constant service disruptions.

However, several vulnerabilities were revealed once the technology was released in the market [24]. A DoS attack was identified over the *Radio Resource Control* (RRC) layer by

Da Yu et al's [25] in 2012. Moreover, the disclosure of the user identity during the initial attachment has been a major concern within the research community since the first release of LTE, proposing numerous methods to tackle this issue [26].

Avoiding service interruptions is crucial on critical situations, where a network disruption could have a severe economical impact or, in the worse-case scenario of a terrorist attack, the cost of human lives. In particular, service availability is extremely necessary for emergency services and first responders Telecom infrastructures, as they must coordinate their actions across different teams, who are located in multiple locations, in a matter of seconds.

The increase on the demand for radio equipment by *Small and Medium Enterprises* (SMEs), and the fast evolution experienced on the microprocessor industry, have made a big impact in the prices of jamming stations. Radio jamming devices are actively used in public spaces, such as theatres, prisons and military basements, where a legitimate isolation of communication services is required to prevent noisy interruptions during a show, guarantee a secured and controlled access to them by the inmates, or preventing any terrorist attack from happenings at a military base, respectively. Off-the-shelf hardware-based and low-cost software-based jammers can be easily acquired in the market for interrupting the communications within a local area at affordable prices [27].

The quick obsolescence of previous technologies has also contributed to the reduction on the prices, by making the construction of home-made jamming stations more accessible at a lower price. All these factors create the ideal environment to make jamming stations affordable not only by companies, but also individuals and radio amateur users. The proliferation of mis-behaved users, who acquire the equipment to perform attacks against commercial and domestic networks with malicious intentions, is inevitable and can only be tackled by strengthening the security measurements.

Nonetheless, corporate networks tend to have a higher awareness of how crucial service availability is and always consider a potential service disruption when planning their business continuity plans and/or assessing business risks. The economical consequences of suffering a service interruption at a critical time makes the prevention of DoS attacks more attractive for corporations and MNOs, demanding additional mechanisms to prevent them from public and private research communities.

1.2.1 Jamming attacks

Jamming attacks are the most efficient method for interfering radio-based communications, using a jammer device to emit on the same radio channel where the data is transmitted. A jammer is a simple radio device, equipped with a transmitter to beam radio signals, designed with the purpose of causing harmful effects on wireless communications.

The immediate consequences of a jamming attack can vary from a light decrease on the network performance to a complete service disruption, depending on the type of jamming attack performed, the emitting power and the duration of the jamming transmission.

In early stages, jammer devices were designed to inhibit communications within an delimited area, broadcasting meaningless data over the communication channel to inflict distortions on the original data transmission due to the collisions. This process is known as physical jamming, as no other layer on the protocol stack is required to perform this attack. However, physical jamming requires constant transmission power over long periods of time, facilitating the traceability of the emitting station and, in some cases, revealing the attacker location.

Intermittent jamming aims at protecting the jammer's location so the attacker is less vulnerable to be identified, reducing also the required power to launch the attack. The beam emissions are performed following preselected intervals or random patterns. However, multiple studies have proven this technique inefficient to prevent jammer tracking, since the transmission interruptions only delays the detection.

The evolution of intermittent jamming is known as intelligent jamming, a more sophisticated jamming method which optimises the energy consumption without affecting the efficiency of the jamming action. In this category, the jammer station takes into account the previous knowledge of how the targeted communication protocol works, and uses it against the communication system to imped any data exchange among the other nodes.

Looking into the particularities of intelligent jammers, it is possible to identify different types of intelligent jamming attacks depending on the property exploited on the communication protocol to jam the radio channel. This thesis focused on the detection of two particular types of intelligent jamming attacks: virtual jamming attacks on IEEE 802.11 networks, and RRC signalling attacks for LTE networks.

The following section provides a more detailed description of every type of physical and intelligent jammers, with a classification on different subcategories depending on the method used to jam the communication channel.

1.2.2 Physical jamming

Physical jamming devices can initially be classified based on the criteria they follow for jamming the communication channel, distinguishing two categories [9]: active or reactive.

Active jammers also known as constant jammers, do not sense the channel before jamming it. Their functionality is reduced to the emission of sense/senseless radio signals through all the time the device is powered on. Depending on the duration of the jamming transmission, physical jammers can be divided into three groups [28, 12]:

Constant jammers

A constant jammer offers the simplest method to disrupt communications by producing constant emissions of meaningless radio signals over the targeted radio frequency band. The complexity of manufacturing this kind of jammers is minimal, reducing their price in the marked and making them easily accessible to malicious users.

On the contrary, constant jamming devices must be provided by dedicated power sources, as the continuous emission of radio signals demand a considerable energy consumption. This characteristic makes them also less practical for malicious users and facilitates the detection due to the easy traceability of radio stations emitting continuously on a static position.

Deceptive jammers

A deceptive jammer requires a bit more of complexity, as this jammer injects a constant stream of well-constructed packages with a valid header, followed by a sense-less payload or no payload at all. The level of energy consumed is similar to a constant jammer, requiring slightly higher computational load due to the construction and validation of the header values. Following the same reasoning, the location of this jammer is easily traceable,as the stream of packages is constant and the emission never is interrupted unless the power source fails.

However, the effects of the traffic injected on the network can be more difficult to detect by the victim nodes, as they are well constructed and will not raise any alarm of suspected behaviour. A deceptive jammer is not considered an intelligent jamming device, since it does not require any deep knowledge about the communication protocol mechanism, and only takes into account the structure of a valid package to replicate it.

Random jammers

A random jammer is an evolution of a deceptive or constant jammer with the aim of reducing the emission periods to save energy, and increase the complexity of being traceable. This type of jammer enables the emissions of meaningful/meaningless packages to the communication channel at random intervals. The duration of the emission also follows a random duration pattern, making the detection by any monitoring station more complicate due to the lack of any pattern in the emission period and duration.

The second category includes the reactive jammers, able to sense the channel and only jam whenever radio activity is detected on it. The aim of this kind of devices is to interfere the legitimate communications by emitting at the same time intervals and frequency/ies of

the legitimate nodes to corrupt their transmissions. This type of jammers consume lower energy levels and are considered more efficient, since they are able to produce the same service disruption but optimising their jamming activity to the specific periods when the network channel is busy.

1.2.3 Intelligent jamming

Intelligent jamming evolved as a natural solution to reduce the probabilities of detection on physical jamming devices. This type of jammers have a deep understanding of the targeted communication protocol, and often require a special configuration tuning depending on the characteristic of the jamming attack implemented. Due to this issue, it is difficult to define a generic sub-classification of all the intelligent jamming types. For the purpose of understanding the two specific attacks studied on this thesis, which fall into this type of jamming, two main groups of intelligent jamming are defined: virtual and signalling jamming. The following paragraphs introduce the most generic characteristics of each type, the particularities of their implementation and the evaluation of benefits and disadvantages.

Virtual jamming

The name of virtual jamming was initially introduced by D. Chen et al. [29] for defining a particular DoS attack tailoring the virtual carrier-sense function of IEEE 802.11. This function was introduced to predict when the communication channel will be occupied and reduce the collisions inflicted by the hidden node problem [30]. The mechanism uses the *Network Allocation Vector* (NAV) value, which is included in most of the frames, as indicator of the time the communication channel will be idle due to a node emission.

Virtual jamming techniques exploit this mechanism by falsely reporting idle periods in the communication channel, causing the rest of the active nodes in the network to initiate the back-off period in which they will not use the channel. This back-off period has a total duration composed of the actual duration reported by the malicious node in the NAV field, and an extra random time to avoid colliding with other active nodes waiting to access the channel.

The jammer will need to initiate at least a short transmission to guarantee the jamming effect success, as all the IEEE 802.11 nodes will compare the virtual availability of the channel against the reported availability while sensing the channel by the physical layer.

Signalling jamming

Finally, the last category of intelligent jamming is named as signalling jamming. This kind of jamming exploits the legitimate use of signalling packets exchanged between the legitimate

nodes and the serving network with the aim of disrupting the communications in the channel. In particular, this thesis studies a specific signalling jamming attack for LTE networks [25], which missuses the mechanism for establishing an RRC connection to perform a DoS attack by flooding the LTE core-network with thousands of connection requests per second.

This type of jamming requires an initial phase of monitoring, when no transmissions are executed, to gain legitimate access to the serving network. Once the required information has been collected, such as IMSI or other type of identification for subscribing nodes, the jamming process will be triggered against the serving network. The jamming activity will remain for as long as required to bring the service down, and the desired time to maintaining the service inaccessible.

1.3 Motivation

Service availability is usually taken for granted, since having a temporary service disruption does not impose a major risk for most of domestic communications. However, radio-based communication services not only provide services to individuals on home networks, but are also used on critical situations by emergency services and first responders, or in military deployments at the battlefield. In addition, wireless communications are the preferred technology used by companies to provide a flexible and secure access to their network services, as discussed during the introduction of this chapter.

A minimal interruption on the communication service could have catastrophic consequences in a temporary network deployment during a natural disaster, or massive terrorist attack, with a cost in human lives. On the contrary, a minimal network outage on a corporate network for a trading company has the potential of causing massive losses in profits, where thousands of transactions are performed every second to optimise capital investments.

This research project aims at addressing current challenges in securing cellular and wireless communications, and contributing to guarantee service availability by strengthening the intrusion detection techniques. Focusing on two major issues affecting the main technologies for future networks, this thesis gives an answer to:

Virtual jamming attack on IEEE 802.11 networks

> This research has identified a set of metrics to detect virtual jamming attacks by analysing the network traffic. Detection results corroborate the efficiency of the proposed algorithm and reveal the most suitable metric combination for reducing the false positive alarms. New ideas are suggested for further research on this matter.

Intelligent DoS attack on 4G networks

A set of metrics is proposed to allow the implementation of countermeasures in the core-network, as part of the rules included in the IDS. The suggested detection algorithm provides an on-line mechanism to identify the attack in real time with a reasonable detection rate and reduced number of false alarms.

1.4 Main contributions

This thesis has contributed to enhance the security of cellular and wireless communications by:

- Identifying a set of metrics based on multiple-layer data fusion for detecting virtual jamming attacks on IEEE 802.11 networks.
- Providing a real test-bed for performing virtual jamming attacks on IEEE 802.11 networks.
- Designating a set of metrics associated with a particular DoS signalling attack for LTE networks.
- Replicating the effects of executing a DoS attack on a LTE emulated deployment with high density on each cell.
- Proposing a new on-line detection system to detect multiple DoS attacks in wireless networks with hight accuracy and low ratio of false positives.

The following chapters provide a completed description of each of the aforementioned contributions, depicting the new enhancements proposed on this research project. It is important to remark the involvement and collaboration of a visiting PhD student, Diego Santoro, as part of an authorised collaboration between Loughborough University and Parthenope University of Naples, Italy.

All the experiments conducted on the Wi-Fi and LTE test-beds were proposed and led by the author of this thesis, but conducted in collaboration with the visiting student. The development of the source-code for implementing the proposed detection algorithm was led by the visiting student, in collaboration with the author of this thesis. The work conducted together has lead to several publications mentioned in Chapter 5. However, all the work presented on this thesis has been individually produced by the author of this thesis, including all the analysis of the datasets collected, the optimisation of the detection algorithm and *Sliding Window* (SW) size for each technology. The presented final conclusions have been carried out individually by the author of this thesis and represented his own ideas.

1.5 Research scope

This thesis focuses on intelligent jamming attacks and detection techniques applicable to wireless communication technologies. The work conducted on this project tackles two specific types of intelligent jamming attacks: virtual jamming on IEEE 802.11 networks and RRC signalling attack on LTE systems. The proposed metrics have no relation among them, offering independent belief sources compatible with *Dempster-Shafer* (D-S) theory of evidence [31].

Despite the fact that results of the proposed detection mechanism are based on traffic measurements collected from a laboratory test-bed, including an emulator on the LTE experiments, conclusions can directly be applied to real infrastructures. Wi-Fi network traffic was collected on a self-designed test-bed composed by real nodes equipped with IEEE 802.11 wireless interfaces, recreating real-life scenarios with multiple nodes.

LTE experiments were initially simulated using OPNET Modeler Suite [32], and later on emulated using equipment manufactured by Aeroflex [33], a leading company on the Telecom industry for providing testing equipment on cellular networks due to the reliability of their products, having a strong support from MNOs and Telecom manufacturers. Both companies, OPNET Technologies Inc. and Aeroflex Inc. have been recently re-branded as Riverbed Technology and Cobham Plc., respectively.

However, this thesis preserves the original company names to guarantee all the software tools and hardware devices mentioned on the experimental phase are accurate. This action removes the chances of confusing the reader when identifying the equipment used on the test-beds, as upgraded or renamed versions of the same products were released after both company acquisitions.

1.6 Thesis outline

The thesis is structured as follows:

Chapter 2 describes the IEEE 802.11 and 3GPP LTE/LTE-Advanced standards for WANs and cellular networks respectively, analysing the main security mechanisms for protecting the data exchange and preventing threats against the service availability. Then, the chapter focuses on the two shortcomings exploited to conduct virtual jamming attacks on each standard: the *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA) mechanism for Wi-Fi networks and the AKA protocol for cellular networks. Finally, the last section introduces the state of art on the existing solutions to tackle the aforementioned shortcomings and detecting virtual jamming attacks, providing an overview of

each proposal and highlighting the pros and cons. Research gaps are identified, leading to the definition of the research scope and challenges faced on this thesis.

Chapter 3 presents the proposed new algorithm to detect DoS attacks in real-time on IEEE 802.11 and LTE/LTE-Advanced networks, providing reliable results with minimal impact on network performance and light computational cost.

Chapter 4 outlines the conducted experiments and test-bed description, with a thorough explanation of all the equipment and configuration required for producing the simulation scenarios. A summary of the initial network traffic is presented, including an analysis of the results after processing the dataset. To conclude, the outcome of executing the proposed detection algorithm is evaluated on each attack, and final conclusions are deducted.

Chapter 5 closes the thesis with a synthesis of this research project, together with a summary of the major contributions and the discussion of potential research directions for future work. Further ideas and improvements are suggested aiming at optimising the current detection algorithm.

CHAPTER 2

Background analysis

2.1 Introduction

This chapter defines the state of the art in the detection and prevention of the two *Denial-of-Service* (DoS) attacks studied on this research project, including a brief assessment of the countermeasures mechanisms proposed by the research community to address them. The analysis of the background, and related literature review, has been split into two different sections to facilitate the comprehension by the reader.

Section 2.2, provides a basic description of the IEEE 802.11 standard[8] and the specific mechanisms required to understand how the virtual jamming attack is carried out to produce a DoS in the wireless network. In particular, the *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA) mechanism is described together with its main vulnerabilities, leading to the explanation of the hidden node problem [34, 30]. Lastly, the *Request-To-Send/Clear-To-Send* (RTS/CTS) mechanism is explained concluding with a summary of the DoS attack studied on this thesis and the solutions suggested by other researchers.

In a similar manner, section 2.3 provides an explanation of the *Long Term Evolution* (LTE) architecture, and the mechanisms involved in the security of the *Radio-Access Network* (RAN). The two mechanisms related with the signalling DoS attack studied on this thesis are presented: the *Authentication and Key Agreement* (AKA) protocol, which acts as entry point for the legitimate users to gain access to the serving network; and the *Radio Resource Control* (RRC) session establishment mechanism, the first step to establish a logical data link between the *User Equipment* (UE) and the serving network. The last part of this section provides an overview

of the suggested solutions to strength these two mechanisms, a critical analysis of them and a short review of the research background.

This chapter concludes with section 2.4 with a brief summary of all the technical information covered on this chapter.

2.2 IEEE 802.11 standard and WiFi networks

The first release of the IEEE 802.11 standard was first published back in 1997 by B.P. Crow et al.[8], as a disruptive technology able to bring radio communications into local networks for business or domestic use. This technology quickly evolved to a commercial standard released in 2012 by the IEEE Standard Association [35]. This initial version included several security mechanism for preserving the security of the information exchanged by adding an encryption layer.

The first encryption mechanism was named as the *Wired Equivalent Privacy* (WEP) protocol, in an attempt to provide robustness to a extremely vulnerable communication radio channel. This protocol was based in the exchange of a secret key shared between the *Access Point* (AP) serving the network and their client hosts. However, it was quickly considered not secure due to its weak RC4 encryption algorithm [36, 37], facilitating the decryption of the secret key by monitoring the network for a short period of time to capture *Initialization Vectors* (IVs) located on the frame header.

The *Wi-Fi Protected Access* (WPA) protocol was the ideal alternative to WEP, offering a more reliable encryption mechanism, while still not offering mutual authentication between client node and AP. Only the AP is able to prove the identity of the client node when the WEP/WPA protocols are used as authentication mechanism. Sadly, this protocol became quickly vulnerable against well-known brute-force and dictionary attacks [38].

The decision of using stronger encryption algorithms was mandatory, relying on bullet-proof encryption algorithms such as *Advanced Encryption Standard* (AES) and *Temporal Key Integrity Protocol* (TKIP), which have not been compromised until now, to preserve confidentiality of the communications over the radio link. These two algorithm were included as part of the WPA2 protocol, also known as IEEE 802.11i [39].

If the three main methods used by the IEEE 802.11 standard to authenticate the client nodes are analysed, it is possible to distinguish between:

Open:

There is no authentication between client node and AP, leaving the communication channel open for any available node in within the coverage area. This authentication

method is not recommended and impose a huge risk of disclosing personal information to any potential attacker.

Shared key: This authentication mechanism provide identity validation of the client node to the AP. However, the client node has no method to prove the authenticity of the serving network. The authentication of each client node is reduced to the possession of the shared secret key. Once the user has been authenticated, the following communications will be authorised by looking at the *Medium Access Control* (MAC) address of the *Wireless Network Interface Card* (WNIC), with the additional risk of suffering MAC spoofing attacks [40].

802.1x [41]:
This authentication mechanism rely on an external server, such a *Remote Authentication Dial-In User Service* (RADIUS) server [42], for validating the authenticity of the client node. The main advantage of this method is the mutual authentication between AP and client node.

The following challenge faced by IEEE 802.11 networks is the management of the access to the radio channel, which is shared between all the active nodes and serving AP associated with the same *Wireless Local Area Network* (WLAN) network or *Basic Service Set Identifier* (BSSID). This responsibility belongs to the CSMA/CA mechanism [30], which manages the access to the medium by establishing the aims at solving the hidden node problem previously mentioned before.

2.2.1 MAC layer and CSMA/CA mechanism

The MAC layer manages the access to the physical radio channel by the upper layers of the protocol stack, regulating the behaviour expected by each wireless node when sharing the channel. This mechanism requires all the client nodes to sense the channel during their transmissions with the aim of detecting any collision should it happens.

The IEEE 802.11 distinguish from physical carrier-sensing function, using information from the physical layer to identify if a collision occurs, and the virtual carrier-sensing function relying on the *Network Allocation Vector* (NAV) field to determine the duration of a transmission. The NAV field is included on the header of most of the control, management and data frames. This parameter should always have as value the time required for completing the transmission of the entire frame, in milliseconds, with a maximum value of 32767 milliseconds[35].

In the event of suffering a collision, the transmitting node should stop the frame transmission and immediately proceed sending a jam signal to inform the rest of active nodes about the

incident. Once the jam signal has been fully transmitted, the node will immediately migrate to idle mode and wait for a random and self-imposed delay time, which includes the back-off time defined by the CW. This back-off time will increase whenever the number of consecutive collisions increases without registering a successful transmission, to reduce the chances of suffering future collisions.

2.2.2 Vulnerabilities and improvements

The main shortcoming identified in the MAC layer is the hidden node problem [30]. This event occurs when two frames collide in the communication channel, but one of the nodes involved in the collision is not able to identify it. Both emitting nodes are within the coverage area of the AP, although they are not within the range of the other node due to the distance.

While the first node detects the collision and transmits the jamming signal, the second emitting node will continue its transmission, keeping the channel busy to transfer a frame already corrupted by the collision. This node will not realise about the collision until the jamming signal reaches its coverage area. However, by the time the node is concious about the recent collision, its transmission will be already completed.

To prevent this phenomenon from happening, the IEEE 802.11 standard defines an additional mechanisms to control the communication channel: the RTS/CTS mechanism. This mechanisms imposes the transmission of a warning messages, named as RTS, with the intention of informing the rest of active nodes about the intention to make a transmission, including the NAV value of the expected transmission. This information is used by the nodes sensing the carrier to estimate for how long they have to wait until attempting to use the radio channel.

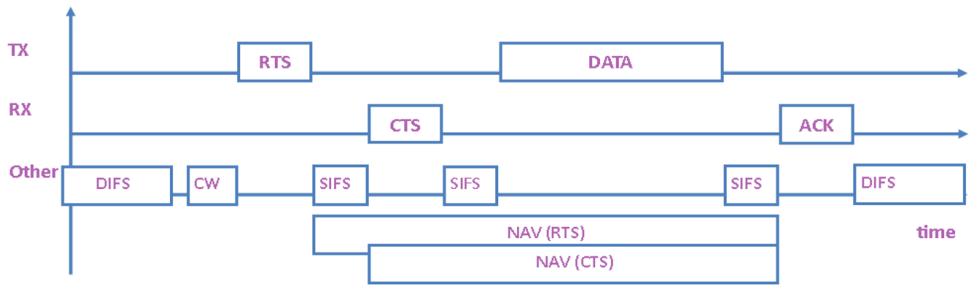


Fig. 2.1 Representation of waiting times for RTS/CTS mechanism [43]

At the end of the transmission, the emitting node will send a CTS frame, to inform about the successful completion of the transmission. Figure 2.1 represent this situation with two nodes attempting to use the communication channel, with the RTS/CTS mechanism enabled. It is important to emphasis on the mandatory implementation of this mechanism for all the

well-behaved nodes, being required to wait for the completion of the emission with a CTS confirmation frame.

The waiting time imposed by the RTS/CTS mechanism on each node also takes into account the *Distributed coordination function Inter-frame Space* (DIFS) and *Short Inter-frame Space* (SIFS) delay. The DIFS is the time required for each node sensing the carrier before being authorise to legitimately transmit a frame. On the other side, the SIFS is the time needed by the receiving node to process the incoming frame, and reply to it.

2.2.3 Virtual Jamming Attack on IEEE 802.11 networks

This attack was initially reported by D. Chen et al. [29], emphasising on its effectiveness to disrupt the service and its simplicity to be carried out. The authors provide a theoretical analysis of the vulnerability, suggesting the definition of three timers to decide whether the incoming frames should be processed or discarded. The first two timers are used to control the RTS and CTS messages, which should always be followed by a data or Acknowledgement (ACK) frame respectively. Using these times, the legitimate node attempting to use the channel will be able to identify the misuse of the channel and automatically ignore the RTS/CTS frames to proceed with its transmissions. The third timer suggested is for the NAV duration reported in the frames, which will allow the legitimate node to transmit whenever the NAV value reported does not match with the expected value for the data transmitted.

The solution proposed has been taken into account when designing the NAV metric used on this thesis, as the duration indicated in the NAV field has been acknowledged in other publications as clear evidence of the attack [44, 27, 45].

Performing the Attack

In order to perform the attack, only two modifications must be carried out in the aforementioned security mechanisms. The first change consist on eliminating the functionality of the Contention Window (CW), which defines the minimum and maximum back-off delay a node should be waiting before attempting to use the communication channel. The implementation of the attack used on this thesis has modified the CW to have a CW_{MAX}=0 and CW_{MIN}=0, setting the duration of the back-off delay to zero for all the collisions detected on the attacker node. The direct effect of this change is that the attacker will automatically start transmitting a new frame without waiting for the radio channel to be idle and free to be used.

The second change on the standard behaviour of a node is produced by the establishment of a fixed value in the NAV field, the maximum value of 32767 milliseconds[35]. Including this NAV field value on every frame transmitted by the attacker will impose unnecessary delays in

the remaining active nodes of the network. The combination of this change with the lack of CW gives the attacker the potential to monopolise the communication channel for as long as the attack is enabled.

The specific software modification used on this thesis to execute the attack are cited in the Appendix C.

2.2.4 Research Background

The study of mechanisms to detect and mitigate jamming attacks has always been an important research area for wireless communications [45, 46, 44, 28, 47, 29]. In this section, this thesis introduces the specific research publications that contributed to define the research path followed on this PhD, and helped on the selection of the candidate metrics for detecting the virtual jamming attack.

The initial publication of D. Chen et al. [29] acted as starting point to characterise the attack and being aware of the potential impact it could have on a Wi-Fi network, as it was previously introduced on section 2.2.3. In addition, other publications extended the analysis of the attack, offering different approaches to mitigate the effects of jamming attacks [48].

The most basic type of DoS attack is the physical jamming, as Chapter 1 explained. A. G. Fragkiadakis et al. [45] proposed a distributed solution to tackle this type of jamming by monitoring the status of the radio channel and the analysis of the Signal-to-Noise Ratio (SNR). The jamming activity is detected either using a threshold or a cumulative sum (Cusum) algorithm. A second version of the algorithm is also proposed, applying Dempster-Shafer (D-S) theory to the outcome of both algorithms. Although this solution improves the results up to 80%, it only uses physical layer metrics making the detection performance sensitive to any normal alteration of the radio signal parameters, such as during network congestion periods.

Complementary to the detection solution, W. Xu et al. [49] present two simple methods to neutralise physical jamming attacks: channel surfing, where the client nodes move to a different communication channel whenever a jamming attack is detected; and spatial retreats, where mobile clients move to safe positions whenever they are victims of a jamming attack (in coordination with the rest of the active nodes in the network).

Using NS-2 simulator, L. Wang et al. [28] managed to evaluate an algorithm that is able to determine the type of jamming attack implemented by monitoring each node within the network. The authors define first the Packets Send Ratio (PSR), or number of packet sent in comparison with the actual number of packet transmissions reported by each node; and the Packet Delivery Ratio (PDR), which compares the number of packets reported as sent against the actual received packets. As final validation, the algorithm uses the signal strength to verify the cases where the PDR might adopt low values as part of a legitimate network activity. This

solution is useful to detect physical and virtual jamming attacks, and is also able to classify the type of jamming being executed, following the classification exposed in Chapter 1. On the contrary, a heavy monitoring on all the node transmissions is required, and it also requires an initial state to set the normal pattern in the signal strength records.

A completely different approach is offered by M. Raya et al. [46], where the software-based solution named DOMINO is presented. The software runs in the AP to be able to monitor the active nodes within the network, and identify rogue behaviours. The DOMINO app is modular and segregates the functions into three components: the Deviation Estimation Component (DEC), the Anomaly Detection Component (ADC) and the Decision Making Component (DMC). In the same manner, this solution also requires of a constant monitoring on all the communications, to analyse variables such as the NAV field, the back-off time and the correct utilisation of the predefined times for implementing the Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) procedure.

The solution proposed by G. Thamilarasu et al. [44] is a distributed system to detect multiple types of jamming attacks looking at metrics from the lower layers of the protocol stack. All the nodes within the network are responsible for monitoring the communications at some point, as the role is randomly assigned. The system looks first at the idle periods in the physical layer, computes the average number of RTS/CTS packets sent by each node, the idle time reported on the NAV field and performed retransmissions. The constant monitoring of these four variables makes this solution not applicable for networks with a big number of active nodes, as the included simulations with GloMoSim confirm. The main novelty is the identification of the CRC errors as valuable metric to determine whether a collision occurs.

The last proposal studied on this thesis is the security mechanism presented by D. Chen [29] to protect the MAC layer protocols. Using timers, the RTS and CTS functions are monitored, together with the NAV virtual idle time reported and implemented. Whenever no new frame is received right after the RTS timer, the algorithm will set the NAV value to zero as a rogue activity has been detected. In the same manner, if a CTS timer expiration is not followed by an ACK packet reception, the NAV timer will be set to zero again to release the channel. The results presented are very positive, since the legitimate nodes barely experience a decrease on the registered throughput during the attack, but this implementation requires of a change in the protocol stack for both network equipment and Wireless Network Interface Cards(WNICs).

The previously introduced publications offer an insight of the variables that could help to characterise the virtual jamming attack studied on this thesis, such as SNR levels, CRC errors, NAV field values, real transmission and reported times when sending/receiving packets and the monitoring of variables related with the CSMA/CA mechanism. Nevertheless, the detection of the specific virtual jamming attack selected on this thesis has not been fully addressed on the

literature review. A lightweight detection algorithm is required to guarantee the applicability in a real on-line Intrusion Detection System (IDS) without any prior knowledge.

2.3 LTE/LTE-A standard and cellular networks

The next generation of mobile cellular networks is aimed at providing high-speed access to broadband mobile services even in the worse scenarios, such as high mobility scenarios, overcrowded cells or rural areas; without detriment to the *Quality-of-Service* (QoS). Additionally, *4th Generation of Mobile Communications* (4G) systems are expected to provide safe communications among a huge number of cellular users, which is growing constantly every year.

The major contribution of the 4G is the portability of the entire network architecture into a flat, all-IP infrastructure where all the services are provided over IP networking and circuit switching is no longer used. This improvement facilitate an easy mobility among different radio-access technologies, such as *Worldwide Interoperability for Microwave Access* (WiMAX), *Wireless Fidelity* (WiFi), *Global System for Mobile communications* (GSM) or *Universal Mobile Telecommunications System* (UMTS), besides making easy backward compatibility with previous technologies.

However, compatibility with heterogeneous access technologies, which are provided by multiple *Mobile Network Operators* (MNOs), produces an increase of the number of hangovers in the RAN. The main consequence of this effect is the mandatory negotiation of strict security policies between the MNOs with the purpose of defining trust policies and authorized users' migration, as well as defining secure countermeasures against identified vulnerabilities.

Since the first release of the *3rd Generation Partnership Project* (3GPP) for the Long Term Evolution (LTE) standard, several publications have pointed out important shortcomings with regards to the security capabilities of this technology[13, 25, 50, 51]. Most of the weaknesses were identified in the RAN, which is the most vulnerable part of the entire system due to its wireless nature and attacks can be easily performed remotely without having physical access to the equipment.

The security capabilities of LTE to protect the radio link are based in pre-defined secure domains with limited scopes and security contexts associated to each user, which are established during the attaching procedure. The security context is built based on a pre-shared master key between the core network and the mobile user or UE, but using additional secondary keys which are dynamically assigned per session to guarantee freshness of the session keys.

The procedure in which the session keys are derived is called EPS-AKA, or Authentication and Key Agreement Protocol for *Evolved Packet System* (EPS), and it is triggered as first

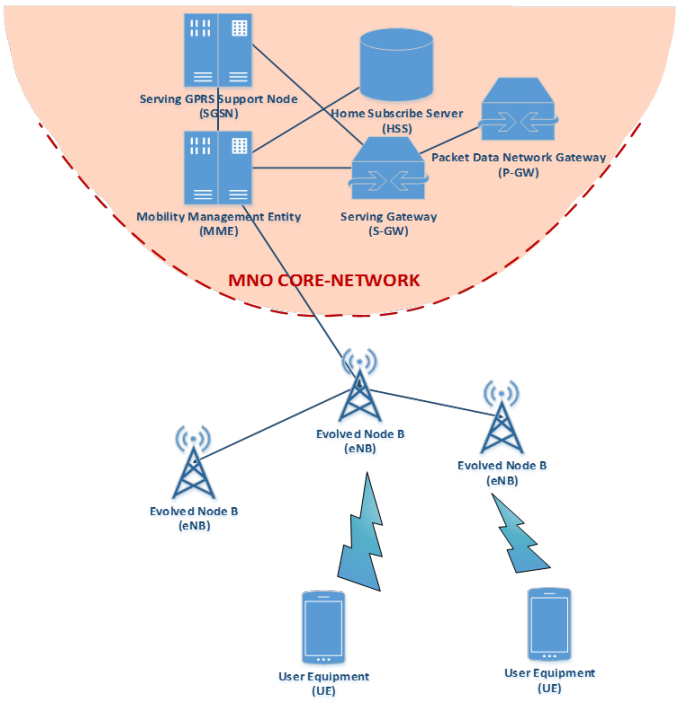


Fig. 2.2 LTE End-to-End Network Architecture

security mechanism during the initial attachment of the mobile device. This protocol plays an important role into the establishment of an initial security context for each user. At the same time, it exhibits most of the identified vulnerabilities of LTE, such as breach of privacy for the user's identity, weak mutual authentication between core-network elements or lack of forward secrecy into the key hierarchy.

This report focuses its interest into the analysis of a particular vulnerability of the EPS-AKA protocol which allows the attacker to perform a DoS attack against the core network. At first, Section 2 describes the vulnerability itself and a wide description of how to perform a local DoS attack over the RRC layer in a pre-selected cell and, to complete it, describes the consequences. Finally, conclusions are stated at the end of the reports, with ideas for further research to strengthen future mobile network communications in LTE deployments.

2.3.1 Authentication and Key Agreement (AKA) protocol

Identification of the user is the first step before gain access to the network. UE establishes contact with the nearest *evolved-Node B* (eNB) triggering the registration process. During the first attempt, *Mobile Management Entity* (MME) is not able to identify the UE by means of a temporary identity (*Globally Unique Temporary Identity* - GUTI), thus, serving network will send an IDENTITY REQUEST message.

A reply message is made by the UE with its *International Mobile Subscriber Identity* (IMSI) transferred in clear text, because no security context has been established before. It breaks the requirements of user identity confidentiality mentioned in the security requirements [52], exposing the user identity to eavesdropping attacks over the radio interface.

Once the MME receives the IDENTITY RESPONSE, GUTI is allocated and paired with the original IMSI. The temporary identity may change for different reasons, being no necessary to transfer the unique subscriber identifier unless serving network can not retrieve it from the GUTI.

Before the establishment of a security context, serving network needs to verify the authenticity of the *Mobile Equipment* (ME), as well as the UE has to verify the serving network. Mutual authentication is achieved by means of an AKA protocol, called EPS-AKA. The process is triggered by the serving network, after the identification success. Figure 2.3 shows the sequence diagram.

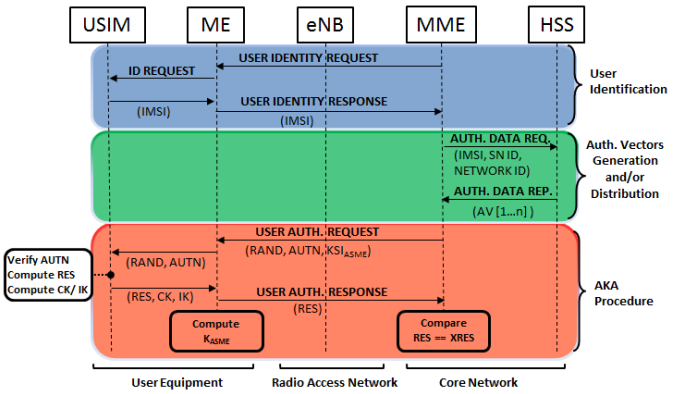


Fig. 2.3 Authentication sequence for *Evolved Universal Terrestrial Radio Access Network* (E-UTRAN)

Initially, MME checks the stored key material and its freshness. If there is any *Authentication Vector* (AV) available it will use it to start the authentication process. If there are no vectors, or the existing ones are no fresh enough, MME will request new AV to the *Home Subscriber Serve*(HSS). Each AV is associated with an IMSI, being only used once per AKA instance. 3GPP recommends to send only one vector on each reply message, but it is not mandatory.

Each AV is composed according to the equation

$$AV := RAND \parallel AUTN \parallel XRES \parallel K_{ASME} \tag{2.1}$$

where each parameter is:

RAND is the challenge to proof the user authenticity.

AUTN is the parameter to proof freshness of authentication vector and serving network authenticity.

XRES is the expected response to the challenge.

$\mathbf{K_{ASME}}$ is an identifier to derives the same key hierarchy in both sides.

The process start with an AUTHENTICATION REQUEST message, composed by an authentication challenge RAND, AUTN parameter to verify the freshness of the key material besides of serving network authenticity, and KSI_{ASME}, a value used by the mobile equipment to generate the same key value for K_{ASME}.

Once the ME receives the message, it retrieves the KSI_{ASME} parameter and passes the other ones to the *Universal Subscriber Identity Module* (USIM). USIM verifies the freshness of the authentication vector, deriving the sequence number from the AUTN parameter. If the derived value match with the expected sequence, a challenge response RES is computed and send back to the UE. Then, two keys are derived from the master key K, one for integrity (IK) and another for confidentiality (CK).

An AUTHENTICATION RESPONSE is sent back to the MME, generating on it the same key pairs CK/IK and completing the AKA process. Now, both extremes are able to generate the same key material, following the scheme of figure 2.4.

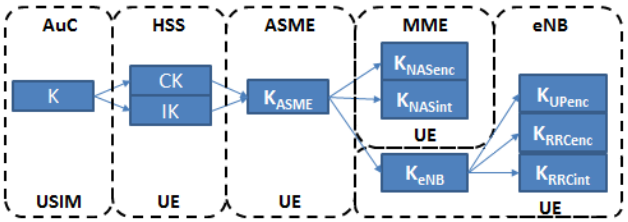


Fig. 2.4 Key hierarchy for E-UTRAN

Each time an AKA process is called, key material is re-generated based on the new value of K_{ASME}. Master key K is securely stored in the HSS and IMSI, without being transmitted or used directly. It is only used to derive the entire key hierarchy.

Access-Stratum and Non-Access-Stratum Security (AS/NAS)

In contrast with UMTS, LTE incorporates a secondary security layer with an extra encryption and hashing level. These two layers are *Access-Stratum* (AS) and *Non-Access-Stratum* (NAS) security. AS security protects the signalling and data traffic between the UE and the eNB, where all signalling messages are confidentially protected by K_{RRCenc} and integrity protected by

K_{RRCint}. User plane traffic is only encrypted using the key K_{UPenc}, leaving integrity protection as free choice of the operator.

On the other hand, NAS security duplicates the robustness of the system against attacks, incorporating another integrity and confidentiality protection for both data flows (signalling and user plane) between UE and MME. The keys used to encrypt and calculate hash codes are K_{NASenc} and K_{NASint} respectively.

DoS in the Radio Resource Control (RRC) layer

The Radio Resource Control layer manages all the functionalities related with the radio interface, negotiating the establishment of the logical channels over the previously assigned radio bearer. It is located in layer 3 and it retrieves all the information about the physical and data link from the lower layer 2, which is composed by three individual sub-layers: *Packet Data Convergence Protocol* (PDCP), Radio Link Control (RLC) and MAC.

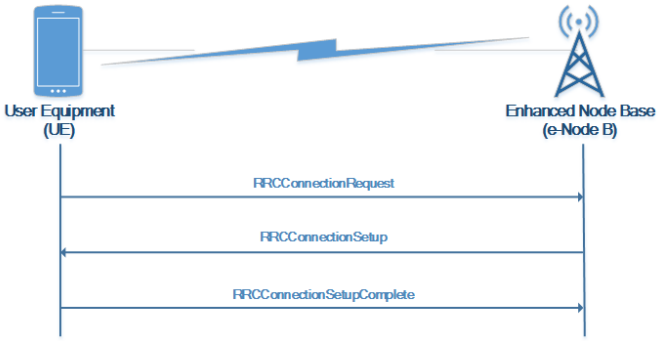
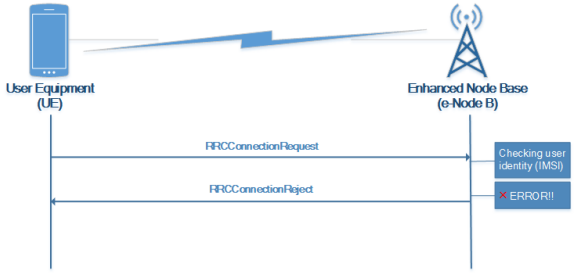


Fig. 2.5 RRC connection data-flow diagram

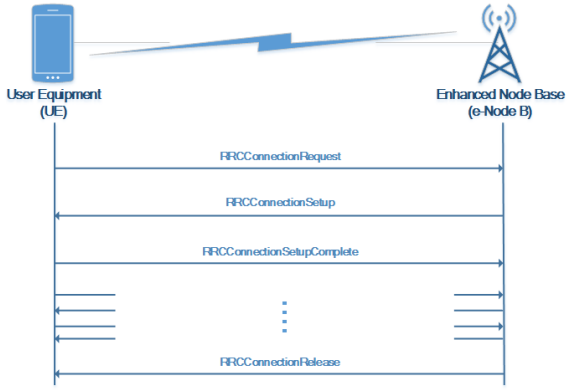
The procedure with which the UE is attached to the core-network as a client requires an initial phase where the designated radio bearer is split into logical channels for the downlink, uplink and control traffic. This process is the RRC CONNECTION establishment, which is precedent to the negotiation of the security context and the initiation of AS/NAS security. Thus, security mechanisms are not enabled until the RRC connection is established since all the security capabilities are implemented over the NAS layer.

Consequently, all the exchanged messages to initiate the process, negotiate the conditions and acknowledge the establishment of a RRC connection need to be transferred in plain-text. These messages are *RRCConnectionRequest*, *RRCConnectionSetup*, *RRCConnectionSetup-Complete*, *RRCConnectionReject* and *RRCConnectionRelease*. Figure 2.5 shows the successful establishment of a RRC connection as it is specified by 3GPP files [53]. The procedure is triggered from the user side by sending the *RRCConnectionRequest* message, opening the gap to missuses from rogue users.

Regarding the status of the mobile terminal, initially the device is in the *RRC-IDLE* status, which only allows the use of *"emergency call"* services. Once the RRC connection is enabled, the status is moved to *RRC-CONNECTED* and all the available services for a particular user are activated.



(a) RRC Connection Rejection



(b) RRC Connection Release

Fig. 2.6 Data-flow diagram for additional RRC messages

The RRC protocol take into consideration the unusual case of having problems during the establishment of the RRC connection, where the MME could reject a *RRCConnectionRequest* if the identity of the user is invalid or any parameter included in the message does not match with the expected value. Then, MME will communicate the rejection by sending a *RRCConnectionReject* message, as figure 2.6(a) shows, and the negotiation will finish. A new instance of a RRC connection need to be started to initiate a new negotiation.

The specifications also contemplate a third case where the eNB or base station can release the established RRC connection in order not to consume unnecessary resources if the RRC connection is not required to be used in the future. In this case, the UE receives a *RRCConnectionRelease* message as it is represented in figure 2.6(b) and it changes from *RRC-CONNECTED* to *RRC-IDLE*.

However, neither *RRCConnectionRelease* nor *RRCConnectionReject* implies any additional threat, since those messages are only sent from the mobile operator side through the eNB.

2.3.2 Vulnerabilities and improvements

In the previous section the functionality of the RRC layer was depicted, pointing out the lack of security before establishing a radio connection. Considering this breach of security, it is possible to use the normal procedure to establish a radio link with the aim of consuming resources to perform a DoS attack. The attack is widely explained in the next section, which is based on the original paper of Yu Da et al. [25].

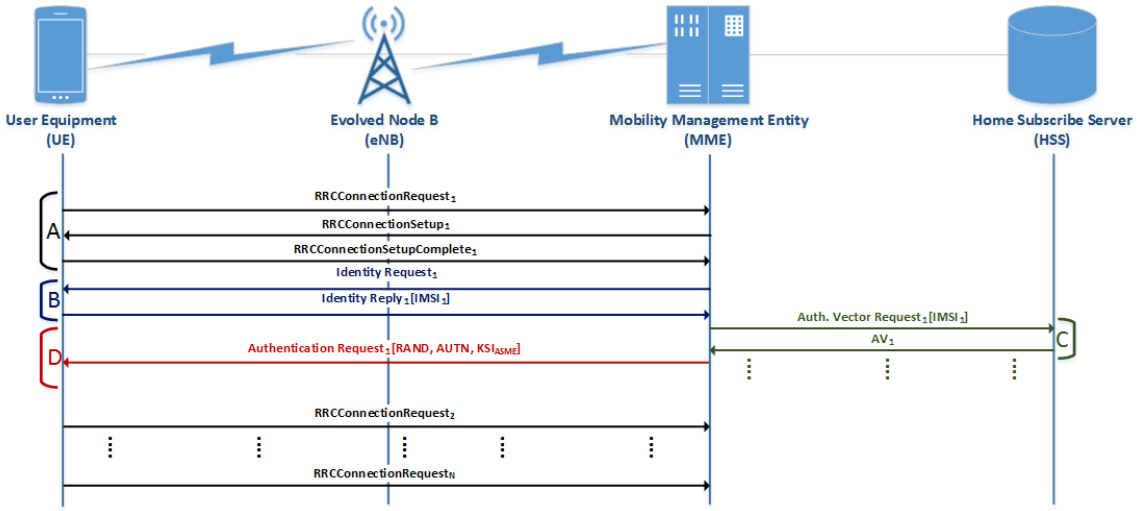


Fig. 2.7 Data-flow diagram of a DoS attack over the RRC layer

In this paper, the authors identified the vulnerability and performed a simulation in a self-implemented tool with the purpose of getting measurements to assess the impact of the attack inside the core network. The results conclude that there is no requirement of having high-computational hardware in order to perform the attack, since it can easily be launched by using a non-sophisticated equipment, such a normal desktop PC. The attack is able to collapse the system in just 30 seconds by using a bunch of legitimate IMSI values which has been gathered previously to send 500 service request per second following a Poisson distribution [25].

The attack exploits a vulnerability in the protocol specifications of the RRC layer of the protocol stack [53], which is at level three of the *Open Systems Interconnection* (OSI) model as shown in figure 2.8. The vulnerability was initially identified by Da Yu et als. [25], and subsequently acknowledged in several publications [24, 54, 55].

Performing the Attack

The aim of this attack is to consume available resources inside the core network by flooding the system with radio service requests which contains legitimate IMSIs previously collected.

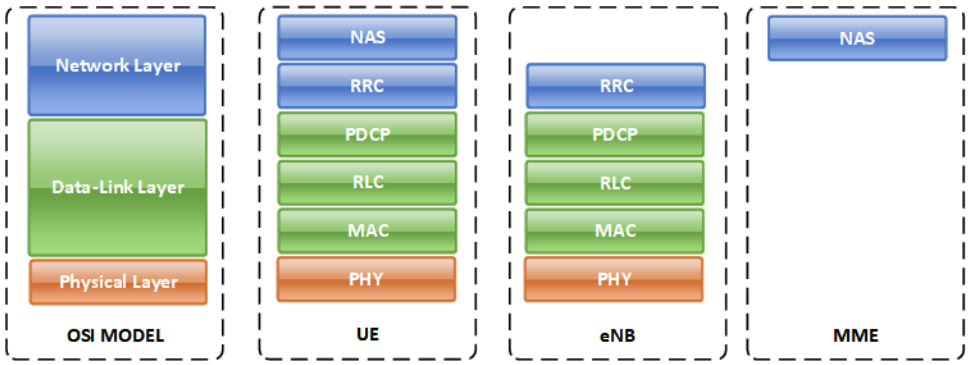


Fig. 2.8 Protocol stack for LTE control plane traffic[56] against OSI model[57]

Initially, the malicious user retrieves legitimate user identities or IMSI from the radio channel by fooling the user to connect with a rogue MME to force the transference of the IMSI with an *Identity Request* message. The attack to gather all the IMSI is widely explained in [58].

Once the attacker has collected enough number of legitimate identities to perform the attack, the second phase is initialised by sending *RRCConnectionRequest* messages including one of the hijacked IMSI. MME receives the service request and retrieves an authentication vector from the HSS. Although MME and HSS validate the user identity by checking the value of the IMSI, the injected message would not be identified as illegitimate message, thus, the authentication process continues as normally.

MME sends a *RRCConnectionSetup* message and launches time trigger waiting for a *RRCConnectionSetupComplete* message which will never arrive. Once the timer is expired, the authentication session is cancelled and all the occupied resources a free.

HSS requires to consume hardware resources, such as RAM memory and CPU usage, in order to compute each authentication vector, as well as storing the derived session keys until the authentication session is completed; or MME manages to detect the attack and the session is cancelled.

The attacker only has to initiate a limited number of *RRCConnectionRequest* simultaneously in order to collapse the available resources of the HSS and block the cell service completely.

In conclusion, this attack has two side effects into the performance of the system. First, the access through the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) in a particular cell, where the attack is being performed, is blocked and legitimate users are isolated since the RAN is inaccessible. Secondly, as a consequence of serving multiple fake service request from the attacker, the core network is driven to the collapse. The collapse occurs due to a heavy computing load registered on the HSS to generate and distribute the authentication vectors.

2.3.3 Research Background

Looking at the work carried out by the research community, two main research lines are clearly defined: the identification and impact assessment of the studied signalling DoS attack, and the enhancements on the AKA mechanism.

The first publication acknowledging the studied signalling DoS attack was presented by Da Yu et al. in 2012 [25], where the authors described the entire process to launch the attack. First, the UE is fooled to transmit the IMSI value instead of using the temporary identity. This action allows the attacker to gather the required list of legitimate IMSIs, and finally perform the signalling attack as explained in section 2.3.2.

Other signalling DoS and intelligent jamming attacks have been identified on LTE networks [59, 60], exploiting the initial allocation of radio bearers to exhaust the resources within the radio cell and disrupt the service. The authors in [59] successfully managed to replicate the attack in an OPNET simulator, and provide a detection mechanism without evaluating its performance thoroughly. However, such type of attacks go beyond the scope for this thesis, which focuses on DoS attacks above the physical layer.

The other line of investigation has focused on improving the existing AKA mechanism proposed by the 3GPP. The disclosure of the IMSI during the initial UE attachment to the RAN is the main vulnerability exploited for performing DoS attacks[61] in LTE networks.

The research community have proposed interesting solutions to deal with this shortcoming, proposing a list of amendments on the original AKA protocol. G.M. Køien's proposed and enhanced AKA mechanism [62] able to provide mutual authentication between RAN and UE. The protocol includes a new concept of USIM card [62], called Enhanced Subscriber Identity Module (ESIM), which is capable of computing pseudo-random values. The new feature enables the generation of challenge requests inside the UE which are used to confirm the identity of the serving network.

However, this solution adds additional computational load to the original radio access procedures, and could impose further challenges when maintaining compatibility with legacy systems.

Xiehua et al. [61] modify the security architecture to act as a wireless public key infrastructure and use digital certificates to confirm identity. The certificates have to be provided in advance to all the entities involved in the authentication process, to be able to gain access to the radio system. This requirement makes more difficult the actual implementation on a real LTE deployment.

A more robust solution is introduced by Yu Zheng et al. [63, 64], combining passwords with fingerprints and public keys to provide full mutual authentication since the initial UE attachment.

Unfortunately, the high computational cost to execute the Diffie-Hellman key agreement and mutual authentication, and the requirement of storing biometric parameters, make its implementation less viable in a commercial deployment.

Due to the aforementioned inconveniences, the author of this thesis believes that further research is required to improve the existing standard of LTE without actually modifying the specification documents. A detection mechanism is required to provide security against signalling DoS attacks while still transferring the IMSI in clear-text whenever the use of temporary identities is not possible.

2.4 Summary

This chapter has covered the technical details involved in protecting the radio channel for LTE and IEEE 802.11 networks. The analysis of each mechanism has revealed a number of weaknesses that can be exploited for compromising the security of the entire communication system. A specific attack has been selected for each technology, to conduct further research experiments and contribute on the early detection of the attacks with a new mechanism.

The selected virtual jamming attack for IEEE 802.11 has proven very effective for disrupting all the communications within a WLAN, impeding the rest of nodes to communicate with the AP. This attack represent a real threat for corporate networks and future 4G/5G systems, where Wi-Fi will be one of the main technologies for facilitating cellular traffic offloading and provide seamless connectivity across heterogeneous RANs.

Several attempts have been able to identify the attack under specific conditions, without tackling real-life situations were multiple nodes behave differently. Additional mechanism should be developed to identify the aforementioned virtual jamming attack and protect the availability of the service. The goal of this thesis is to identify some of the meaningful metrics suggested on the literature review and propose new ones to better characterise the attack, facilitating its on-line detection with high accuracy.

The RRC signalling attack for LTE becomes an important vulnerability in LTE systems, which has to be taken into consideration for future releases of the standard specification versions. Although the targets of the attack are specific segments of the network, and must be performed within a short-distance to the serving network to target an specific cell, it has a direct effect into the entire core-network of a particular MNO.

Due to this issue, the author consider as a priority to face this vulnerability by identifying metrics from multiple layers which might be useful to detect an attack in real time, and provide countermeasures to block it without having a real impact in the QoS of the legitimate users.

The aim of this thesis is to identify suitable metrics from the traffic generated through software-based simulation tools and hardware-based emulators, such as OPNET [32] and Aeroflex equipment [33], with the purpose of implementing them in an Intrusion Detection System for LTE networks. These metrics should be accurate enough to detect the attack in real time with a minimal false-positive ratio.

Strengthening cellular and wireless communication systems is crucial to guarantee the availability of the service, a crucial requirement in particular scenarios where these attacks would be specially harmful, such as terrorism, first-responder communications, domestic burglar alarms, or any other criminal actions which could benefit from isolating the victim network for a short period of time.

CHAPTER 3

Proposed detection methodology

3.1 Introduction

This chapter depicts the detection methodology used on this thesis for processing the experimental dataset for both the *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 and *Long Term Evolution* (LTE) experiments. It is important to remark that the first version of this algorithm was initially published by F.J. Aparicio et al. [65, 66], and adjusted to be applied to multiple types of attacks for *Wireless Fidelity* (Wi-Fi) networks, such as: *Man-in-the-Middle* (MitM) and disassociation attacks.

However, the new version applied on this thesis has been readjusted to be compatible with the proposed metrics, and able to address the particularities of the two *Denial-of-Service* (DoS) attacks studied. Moreover, this algorithm has never been applied to LTE network traffic to the best knowledge of the author of this thesis, having no reference on its efficacy with the traffic patterns registered on cellular networks.

The following section 3.3 explains the proposed detection algorithm, and all the mechanisms involved on the process from the live collection of the metrics to the final phase, where all the sources of evidence are fused into a final decision.

Finally, section 3.4 presents the core part of the detection algorithm: the metrics. A list of five metrics are introduced for detecting virtual jamming attacks in wireless technologies, followed by the description of three additional metrics designed for identifying *Radio Resource Control* (RRC) signalling attacks in LTE cellular networks.

The chapter ends with a brief summary in section 3.6, where the main topics covered on the previous sections are highlighted, leading to the introduction of Chapter 4, where the actual results of applying this detection algorithm are presented.

3.2 Dempster-Shafer Theory

In order to understand the proposed algorithm, it is necessary to introduce first *D*empster-Shafer (D-S) theory of evidence[31]. This technique is used to fuse the information collected from different observers about the same events. The observers on this thesis are the proposed metrics. The total number of possible events are grouped into the Frame of Discernment, represented on formula 3.1, which creates a finite set with all the possible mutually exclusive responses about an specific problem.

$$\Theta = \Theta_1, \Theta_2, ..., \Theta_n \tag{3.1}$$

The Frame of Discernment allows the elaboration of hypotheses, or subsets of Θ, having a maximum number of mutually exclusive subsets defined by the power set. The formula to represent the power set is as follows:

$$P(\Theta) = 2^{\Theta} \tag{3.2}$$

It is important to remark that the empty set (ϕ) is always part of the power set. Any of the subsets defined by the intersection of different responses, or elements of Θ, are considered uncertainty, as there is not enough evidence to prove a single hypothesis as valid.

Applying the theory of evidence, probabilities are assigned to each of the hypothesis, using the following mass probability function:

$$m : 2^{\Theta} \rightarrow [0, 1] \tag{3.3}$$

The main difference between the theory of evidence and the probability theory is that the additivity rule is no longer applied when computing the beliefs. The resulting probability will always fall within the following confidence interval [31, 67]:

$$[\sum_{A \subseteq H} m(A), 1 - \sum_{A \cap H = \phi} m(A)] \tag{3.4}$$

where

A is the perception of the observer providing the evidence.

The assignment of probabilities must follow these conditions[31]:

$$m(\phi) = 0 \tag{3.5}$$

$$m(H) >= 0, \forall H \subseteq \Theta \tag{3.6}$$

$$\sum_{H \subseteq \Theta} m(H) = 1 \tag{3.7}$$

where

$m(\phi)$ is the probability of the empty set, always equal to zero.

$m(H)$ is the probability for the hypothesis H.

$\sum_{H \subseteq \Theta} m(H)$ is the overall probability of all the hypotheses included in the set (Θ).

Once a probability has been assigned for all the hypotheses, the rule of combination[31] defines the method to combine evidences from multiple observers about the same event. The fuse of evidences is only possible whenever all the observers are facing the same problem and set of events/hypotheses, as mentioned before. In essence, this condition requires for all the observers to share the same Frame of Discernment.

The rule of combination is applied to fuse beliefs of two independent observers into a common belief, and it is defined by the following formula:

$$m_{comb}(H) = \frac{\sum_{X \cap Y = H} = m_1(X) * m_2(Y)}{1 - \sum_{X \cap Y = \phi} = m_1(X) * m_2(Y)} \forall H \neq \phi \tag{3.8}$$

where

$m_{comb}(H)$ is the probability of the hypothesis H, obtained as a result of fusing into a single belief the probability assigned by two independent observers for the same hypothesis H.

X, Y are the two different perceptions produced by each observer about the same event.

$m_1(X)$ is the probability associated with the hypothesis X perceived by the observer 1.

Since this rule can be generalised by iteration [67], the resulting belief can be used as new source of evidence for the same problem. Reducing the number of observers to only two on each iteration keeps the computational cost of the D-S process low. The proposed detection algorithm combines the evidences collected from multiple metrics by consecutively applying the rule on each key pair. The outcome of combining the first two metrics is used as new belief, being possible to apply again the rule including a third metric as second input on the next iteration.

3.3 Detection Algorithm

In order to understand the mechanism used on this thesis for detecting DoS attacks, it is important to define the sources of information used to feed the entire detection process. All this information is captured by constantly monitoring the activity of the network to extract the required metric information. Figure 3.1 describes the general view of the entire detection process, where it is possible to identify four main zones:

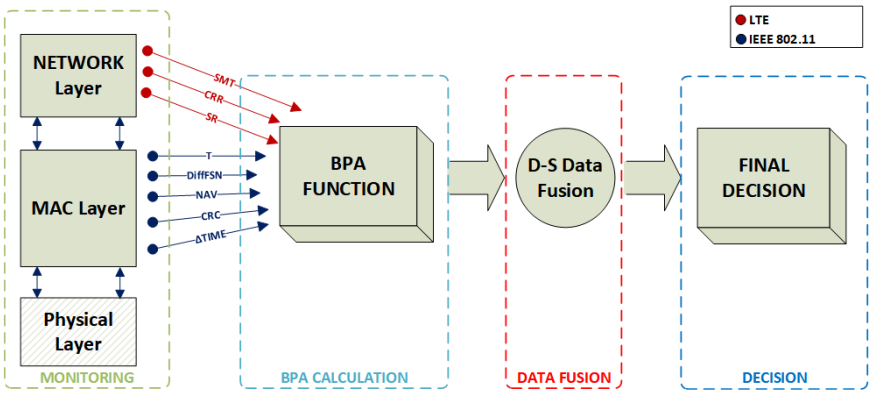


Fig. 3.1 General view of the detection process

1. **MONITORING ZONE:**
   This phase is represented on the left side of figure 3.1, where the *Open Systems Interconnection* (OSI) model of the protocol stack is represented. The proposed metrics are mentioned, indicating from which layer the information is extracted to compute them: Physical, MAC or Network layer. LTE metrics are indicated in red colour, coming from the Network layer, while the IEEE 802.11 metrics are marked in red colour and are computed with information extracted from the MAC layer.

   The outcome of this phase will be a single buffer for each metric, containing the individual samples collected from the network traffic for each monitored metric.

2. **BPA COMPUTATION ZONE:**
   During this phase, the statistical parameters are computed using a sliding window with a pre-defined size. These values are introduced into the *Basic Probability Assignment* (BPA) function together with the original metric samples from each frame, producing the BPA values on each buffer for the three evaluated hypothesis: normal, attack and uncertainty. The outcome of this phase will be three different buffers containing a BPA value for each frame and evaluated hypothesis.

3. **DATA FUSION ZONE:**
   During this phase, the individual buffers obtained during the BPA computation phase are fused, using the outcome of each data fusion as new input to be merged with the next metric. *Dempster-Shafer* (D-S) theory [31] is used to merge the two sources of evidence on each iteration for the three hypothesis, creating three output buffers with all the belief predictions obtained from the fusing process. A triplet of beliefs for each frame will be the final outcome of this phase.

4. **DECISION ZONE:**
   The last part of the process is the final decision, in which the resulting beliefs in Attack, Normal and Uncertainty are received, selecting the hypothesis with the highest probability, or uncertainty whenever the probability matches for both Attack and Normal hypotheses.

The aforementioned explanation of the detection algorithm only provides a general view of the overall process, requiring a more detailed analysis of each phase to better understand how it works. The detection algorithm is composed by six principal steps, covering all the stages of the detection process since the initial monitoring of the network up to the final outcome of the algorithm, where the beliefs are fused and the final prediction is communicated.

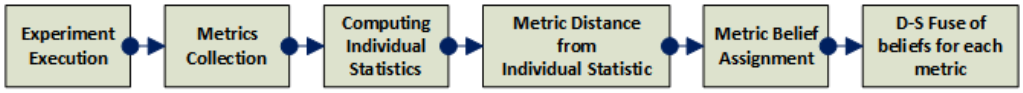


Fig. 3.2 Phases of the detection methodology proposed

Figure 3.2 reveals a more detailed view of each zone previously introduced. The following sections depict all the actions to be executed on each phase, the logic hidden behind the input data sources of each phase and the produced outcome. The rest of this section analyses each of these actions individually, with additional figures to support the explanation. Although the following figures have been created using the metrics for the *Wireless Fidelity* (Wi-Fi) experiments as example, the detection process is executed in the same manner for the LTE experiments.

3.3.1 Collecting Selected Metrics

The collection of the metric samples is produced by analysing the field values of every frame captured during the duration of the monitoring phase. The required information for computing each metric is collected by individually analysing the frames in the dataset.

Using the specific formula of each metric, the metric values are computed for every frame. The outcome of this phase is a sorted buffer composed by multiple time slots. Each time slot

contains a vector with the resulting values for each metric on that particular time slot. The buffer is sorted using the timestamps included on every frame.

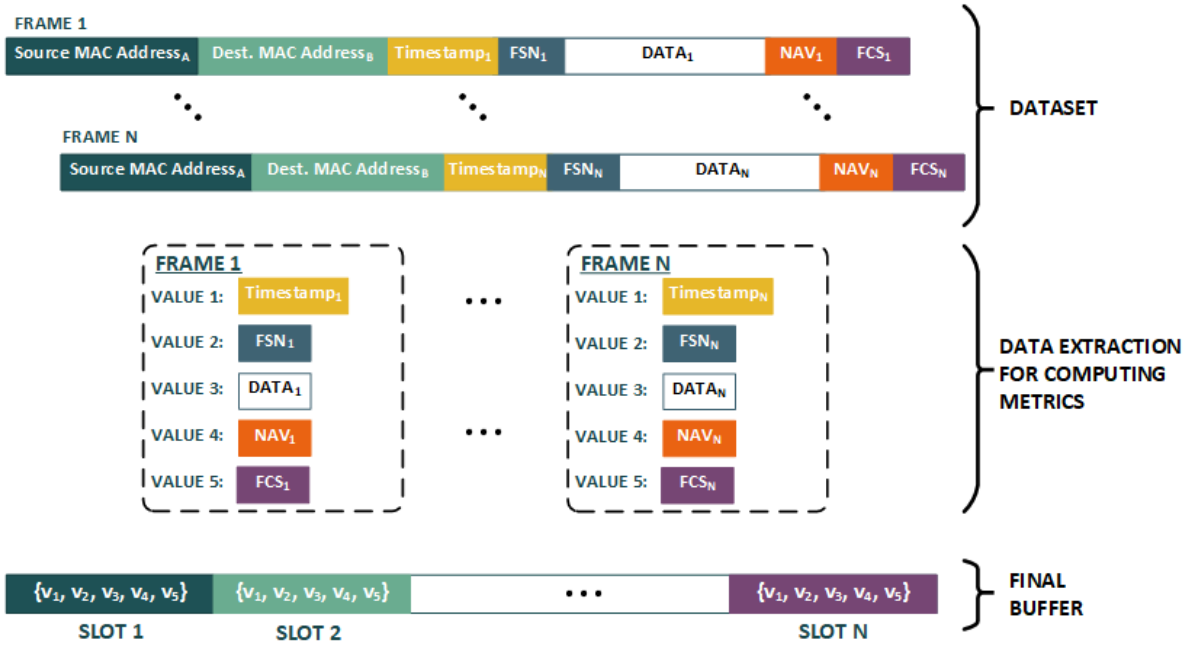


Fig. 3.3 Process for collecting the metric values

For the purpose of validating the detection algorithm proposed on this thesis, the actual execution of this phase was divided into two sub-phases. First, the experiments were conducted while a passive node was constantly sensing the channel and capturing all the traffic transferred through it. Once all the traffic was collected into a *Packet Capture* (PCAP) file, an off-line metric collection process was executed for computing the metrics previously introduced on Chapter 2 and creating the aforementioned buffer. Each time slot of the final buffer was tagged as malicious or normal, since having a labelled dataset was crucial for being able to identify how accurate the detection algorithm is.

3.3.2 Computing Statistical Parameters

Once all the metric samples are collected and ready to be processed, the next step is computing the desired statistical parameter to build the normality pattern and identify the anomaly values within the sample.

The analysis of a single sample does not provide evidence of any event happening in the network, unless this sample is compared against other samples from the same metric. In this phase, the concept of *Sliding Window* (SW) is introduced to construct the relational pattern between the samples, as shown in figures 3.4.

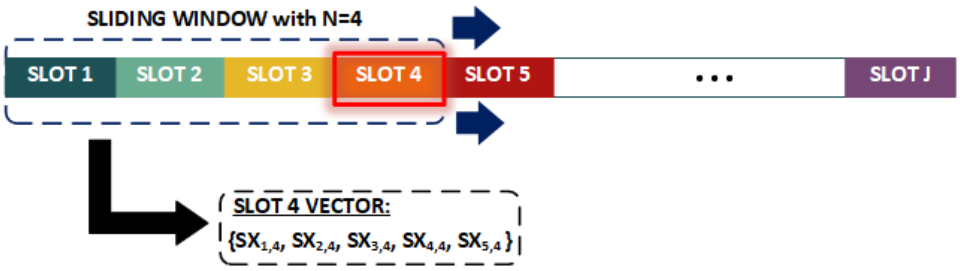


Fig. 3.4 Process for computing the statistical parameter - Iteration 4

The SW is a *First-In/First-Out* (FIFO) buffer, with a predefined fixed size, that slides across the samples buffer to group them. By grouping them, it is possible to compute the desired statistical parameters to build the relational pattern across the same type of samples.

This thesis has selected the mean value $\bar{x} = \frac{\sum x}{n}$ as reference statistic parameter, which is a clear indicator for building the normality pattern of the collected network traffic. The mean is computed for every time slot of the metric samples buffer, on each metric of the slot. Once the mean has been obtained for every time slot, the value will be used to compute additional parameters and finally obtain the beliefs on the next stage of the detection process.

Using the value of the metric on that particular time slot, and the historical values of the same metric included within the SW, the statistical parameters are computed and placed in a temporary buffer. The statistical parameters are computed following this formula:

$$SX_{i,j} = \frac{\sum_{x=1}^{j+n-1} v_i(x)}{n} \tag{3.9}$$

where

$SX_{i,j}(x)$ is the statistical parameter for the metric 'i' collected on the time slot 'j'.

$v_i(x)$ is the value of the metric 'i' in the slot time 'x'.

n represents the number of slots contained within the SW.

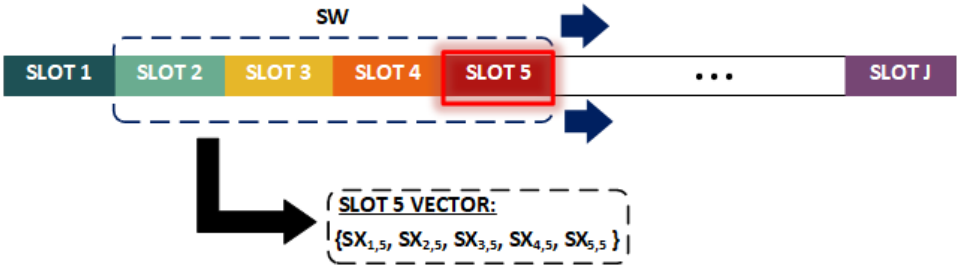


Fig. 3.5 Process for computing the statistical parameter - Iteration 5

In the first iteration of the SW, the time slot 1 will obtain the same statistical parameter as the metric value on that time slot, since there are no previous records or historical samples. However, any future iteration of the SW will contain new time slots, as seen in figure 3.5. During the sliding process, the SW is moved one slot forward per iteration, causing the variation of the final statistical parameters computed on each slot.

Following the example on the analysis of the WiFi experiments, if the statistical parameter is computed for the metric 1 on the forth SW iteration, which is represented in figure 3.4, the obtained result would be as follows:

$$SX_{1,4} = \frac{v_1(1) + v_1(2) + v_1(3) + v_1(4)}{4} \tag{3.10}$$

The initial buffer of samples obtained on the previous phase leads to the generation of the temporary buffer with all the statistical parameters, which is composed by recursively applying this process on each slot. Both the main sample buffer, and the temporary buffer with the statistical parameters have the same number of slots.

Once the statistical parameters have been computed for all the possible iterations of the SW, the temporary buffer will contain now a vector on every time slot matching the following formula:

$$\{SX_{1,4}, SX_{2,4}, SX_{3,4}, SX_{4,4}, SX_{5,4}\} \tag{3.11}$$

In this example, the vector contains 5 elements, which is the equivalent number of metrics used for the analysis of the Wi-Fi experiments taken as reference for explaining the algorithm.

3.3.3 Evaluating Distance from Reference Value

Using the temporary buffer computed before, this phase measures the distance between the current sample registered in the main metric sample buffer, and the normality pattern already built on the temporary buffer.

On this thesis, the distance from the reference statistical parameter is computed following the approach indicated by F.J. Aparicio et al. [66]. In this publication, the authors define the angular mean for computing the belief in Attack, and a pre-defined linear scale with multiple ranges for selecting the belief in Normal.

During this stage, the variables required to apply the formulas for the aforementioned beliefs will be computed, using the temporary buffer with the statistical parameters obtained on the previous stage. The actual method to compute the beliefs in Normal/Attack/Uncertainty, and assign the final probability to each hypothesis, is defined as Belief Assignment.

3.3.4 Belief Assignment

Using the values computed on the previous phase, the beliefs are assigned to each metric sample included in the main buffer. The following paragraphs explain the process in detail.

Belief in Normal

The belief in Normal is computed by composing the BPA scale for the selected metric and the metric values included on this iteration of the SW. The scale follows the well-known statistical method for descriptive analysis of samples, called 'box and whisker' [68], which helps to detect anomalies in the group of samples by analysing the distribution of samples within it.

The quartiles are computed for all the frames included on the SW, using the Q_2 as the range with the highest probability in Normal, as this value represent the Mean of the group. The first and third quartile are also used to compute the *Minimum* (Min), *Maximum* (Max) and *Interquartile Range* (IRQ) values of the sample group, following the formula indicated by this statistical method:

$$Min = Q_1 - 1.5 * IQR \tag{3.12}$$

$$Max = Q_3 + 1.5 * IQR \tag{3.13}$$

$$IQR = Q_3 - Q_1 \tag{3.14}$$

Using this statistical method, any value lower than the Min value, or higher than the Max value will be considered an anomaly. To compute the belief in Normal $BPA_N(x)$ for that specific time slot and metric sample, the sample value is evaluated, obtaining the probability indicated in the list depending on which one of the intervals the sample falls into. The closer the sample value is to the edge cases (Min and Max values), the lower the probability assigned to it is. In the same manner, the closer the sample value is to the mean value (Me), the higher the probability assigned to it is. The ranges are defined as follows:

- $v_i(x) \in [-\infty, Min) \Longrightarrow BPA_N(x) = 0.15.$
- $v_i(x) \in [Min, Q_1) \Longrightarrow BPA_N(x) = 0.3.$
- $v_i(x) \in [Q_1, Me) \Longrightarrow BPA_N(x) = 0.4.$
- $v_i(x) = Me \Longrightarrow BPA_N(x) = 0.5.$
- $v_i(x) \in (Me, Q_3] \Longrightarrow BPA_N(x) = 0.4.$
- $v_i(x) \in (Q_3, Max] \Longrightarrow BPA_N(x) = 0.3.$

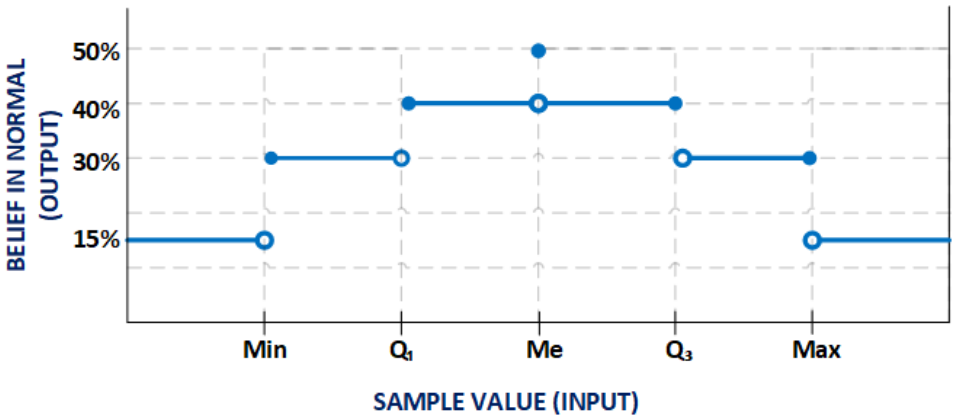


Fig. 3.6 Assigning Beliefs in Normal

- $v_i(x) \in (Max, +\infty] \Longrightarrow BPA_N(x) = 0.15$.

The author of this thesis has used the same range definition used by F.J. Aparicio et al. [65, 66], as it follows a fair probability assignment depending on the distance from the average value (Me) taking into account the distribution of the total number of collected samples.

Belief in Attack

In the process for computing the belief in Attack $BPA_A(x)$, the automated BPA function considers two statistical parameters: the Euclidean distance of the sample value on the current frame, and the frequency of the sample values within the current iteration of the SW. The method proposed in [66] merges both parameters by following these steps:

- First, this method calculates the highest number of times a sample value is repeated within the SW, defining it as *Frequency* (F), for the total n samples within the SW.
- Using the *Mean* (Me) of the n samples within the SW, this method computes the angle α generated by the frequency, represented in the Y axis, and the value with the largest *Euclidean distance* (D_{max}) from the Me, which is represented in the X axis defining a triangle between the two vectors (F and D_{max}). The triangle is represented in blue on figure 3.7.
- The D_{max} is calculated by comparing the current sample value against the maximum and minimum values registered on the current SW iteration. The D_{max} will be the maximum value when comparing the distance from the sample value to the maximum value in the SW, and the distance from the minimum value to the sample value. The D_{max}) value will always be a positive number.

- For each evaluated sample, the system calculates the β angle as indicated in formula 3.15. This angle draws a second triangle, represented in green on figure 3.7, composed by the original F vector and the *Distance* (D) from the sample value (represented with the red dot in figure 3.7) to the Me value of the SW.

- Finally, the resulting β angle is compared against the original α angle, and the belief in Attack is computed as follows:

  If β >= α: 50% probability in Attack is assigned.

  If β < α: the probability in Attack is defined by $\frac{\beta}{2*\alpha}$

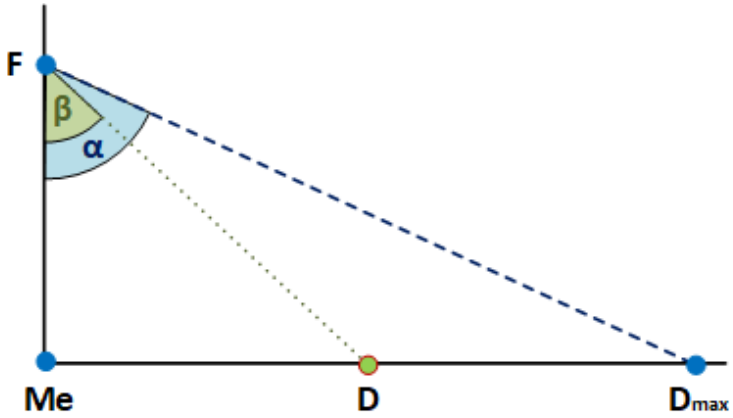


Fig. 3.7 Assigning Beliefs in Attack

$$\beta = cos^{-1}(\frac{F}{(D^2+F^2)(\frac{1}{2})}) \tag{3.15}$$

Belief in Uncertainty

Finally, the last belief to be computed is the belief in Uncertainty, which is computed taking into account the two belief already obtained on the previous steps. This belief does not require of any additional algorithm to be computed, since it is deducted from the two beliefs previously obtained in the same manner the original authors did in the references [65, 66]. The formula 3.16 to calculate its value is:

$$BPA_U(x) = \frac{Min(BPA_N, BPA_A)}{2 * Max(BPA_N, BPA_A)} \tag{3.16}$$

where

Min(BPA_N, BPA_A) represents the value of the belief with the lowest probability (belief in Normal or in Attack).

Max(BPA_N, BPA_A) represents the value of the belief with the highest probability (belief in Normal or in Attack).

Beliefs Adjustment

In the event of registering the maximum value for the belief in Attack and the belief in Normal, which is set to 0.5, it would not be possible to estimate how much uncertainty exists without breaking the rules defined to apply D-S theory. The overall probability of the *Frame of Discernment*, which includes any subset of events that could lead to an hypotheses, must be equal to 1. The solution to meet this requirement is adjusting all the beliefs to avoid overpassing the maximum value of 1 when the probability of any subset is aggregated in the frame of discernment. The correction factor, named as Ψ when first presented by F.J. Aparicio et al. [65, 66], is defined as:

$$\Psi = \frac{(BPA_N + BPA_A + BPA_U) - 1}{3} \tag{3.17}$$

The final outcome of this phase is a probability value for each hypothesis on the current time slot, after applying the correction factor to the three probabilities:

$$BPA_N = BPA_N(x) - \Theta \tag{3.18}$$

$$BPA_A = BPA_A(x) - \Theta \tag{3.19}$$

$$BPA_U = BPA_U(x) - \Theta \tag{3.20}$$

Once the correction factor is applied, the algorithm complies with all the requirements for applying D-S. This factor guarantees a maximum value when evaluating the overall probability for all the subsets within the frame of discernment. However, the method used to compute the correction factor does not compromise the independence for the three hypothesis observed.

The proposed algorithm evaluates three independent hypothesis with no relation between then, and only applies the correction factor to equally reduce the estimated values of each hypothesis before applying D-S theory.

3.3.5 Data Fusion

The process of combining the individual beliefs computed for each metric is named as data fusion. This algorithm applies the D-S theory [31] to combine the selected metrics in groups

of two. This theory has been applied to anomaly detection in the past [67, 45, 69, 65, 70, 71], enhancing the individual results of multiple sources of evidence.

The process begins by defining the frame of discernment with all the possible independent results of the studied problem. In the attack detection process, the proposed algorithm considers the following results:

$$\Theta = \{Attack, Normal\} \tag{3.21}$$

Once the frame of discernment has been defined, the next step is considering all the possible mutually exclusive hypotheses available on this scenario:

$$P(\Theta) = 2^{\Theta} = \{\phi, Attack, Normal, Attack|Normal\} = \{\phi, Attack, Normal, Uncertainty\} \tag{3.22}$$

It is important to remark that the process followed to compute the probabilities on each of the three hypothesis meets the conditions previously introduced in section 3.2:

$$m(\phi) = 0$$

$$m(Attack), m(Normal), m(Uncertainty) \in [0,1]$$

$$\sum_{A \subseteq \Theta} m(A) = m(\phi) + m(Attack) + m(Normal) + m(Uncertainty) = 1$$

The calculation of the mass probability function defined by the theory of combination for two of the proposed metric would be obtained evaluating the formula:

$$m_{comb}(H) = \frac{\sum_{X \cap Y = H} = m_1(X) * m_2(Y)}{1 - \sum_{X \cap Y = \phi} = m_1(X) * m_2(Y)} \forall H \neq \phi \tag{3.23}$$

where

$m_{comb}(H)$ is the probability of the hypothesis H, obtained as a result of fusing into a single belief the probability assigned by the two metrics for the same hypothesis H.

This process will be repeated recursively, combining the resulting belief with the remaining metrics.

3.4 Proposed metrics for DoS on WiFi networks

This section introduces the metrics proposed for detecting the DoS attacks studied on this thesis, as a result of the information collected during the background analysis and literature review. First, five metrics are presented in section 3.4.1 to detect the virtual jamming attack for IEEE 802.11 networks, covering the information extracted from two layers of the IEEE 802.11 protocol stack: MAC and Logical Link Control (LLC) layers. These two layers are the equivalent to the second layer in the OSI model [57], the *Data Link* (DL) layer.

Each metric has a long name, which is more descriptive to intuitively understand how it is computed. Furthermore, a short name is also assigned to each metric, indicated between brackets, which is used in all the following sections of this thesis to reduce the space required and make easier for the reader to understand all the explanations.

3.4.1 Metrics definition

The virtual jamming attack has been characterised using 5 metrics from the MAC layer: Frame Check Sequence Error Rate (CRC), Frame Duration Difference (NAV), Inter-arrival Time (Δ Time), Sequence-Number Diference (DiffFSN) and Throughput Rate (T). These metrics are computed as follows:

Frame Check Sequence Error Rate (CRC)

The *Frame Check Sequence* (FCS) is a value included on each frame to validate the consistency of the data transmitted on it. Looking at the number of FCS error rate, it is possible to identify the healthiness on the data delivered within the WiFi network and uncover unusual activity patterns or high number of collisions.

The errors detected by the FCS might be caused due to several reasons: collisions in the communication channel, hardware issues with the *Wireless Network Interface Card* (WNIC)/cable/socket or incorrect generation in the source node.

Frame Duration Difference (NAV)

The IEEE 802.11 standard defines the *Network Allocation Vector* (NAV) as the time required for a station to completely transmit a specific frame. This estimated value is considered the frame duration, and should always be close to match the real time required to complete the transmission of a frame.

The DoS attack investigated on this thesis has a direct relation with the NAV value, as the attacker will always report the longest duration on the NAV value while transmitting data

frames with a shorter duration. The proposed metric computes the difference between the NAV value indicated within the frame and the actual duration of the frame transmission in milliseconds. This value has been directly referred to NAV on this thesis.

The short name assigned to this metric does not represent the actual NAV field value included within the header of the MAC messages, and will always be cited as NAV metric in the following sections, to avoid confusing the reader.

Inter-arrival Time ($\Delta Time$)

The inter-arrival time is defined as the time difference between the arrival of two consecutive frames to the same node from the same sender. This time is an indicator of the traffic load inflicted by a single node on an specific host. Once the attack is active, this metric is expected to increase, as the transmissions slots are coped by the jamming station reducing the chances of successful legitimate transmissions and, consequently, increasing the time between the arrivals of consecutive messages.

Sequence-Number Diference (DiffFSN)

The *Frame Sequence Number* (FSN) is a numeration used to identify the sequencing of each frame in the time scale. During a normal transmission, FSN values are expected to have consecutive values on each radio link, unless any frame is lost or discarded at reception due to data corruption. Looking at the difference between each data frame exchanged between each node and the *Access Point* (AP), this metrics is able to reveal the lost of data frames due to normal network congestion[49] or as consequence of a DoS attack coping with most of the resources.

Throughput Rate (T)

As the name indicates, this metrics is the equivalent throughput rate registered by each node on every sampling slot. This metrics belongs to the *Physical* (PHY) layer, making it very sensitive to any changes produced on the physical communication channel such as physical obstacles between node and AP affecting the radio signal characteristics, external radio interferences, or the variations in the number of nodes competing for the same radio channel. However, this metrics represent the most reliable figures to verify the side effects of a DoS, expecting abrupt decreases on the registered throughput whenever a DoS attack is launched.

3.5 Proposed metrics for DoS on LTE networks

Once the Wi-Fi metrics have been explained, three new metrics for detecting the RRC signalling DoS attack in LTE networks are presented on this section. The three metrics have been specially designed by the author of this thesis to characterise the particularities of the DoS attack studied, being used for first time to target this attack to the best knowledge of this author.

All the metrics used for detecting the signalling attack are extracted from the same layer in the LTE protocol stack [56], the RRC layer. Following the same reasoning described in section 3.4, every metric presented on this section has a more descriptive long name, and the actual name used across the different chapters of this thesis, which is mentioned between brackets.

3.5.1 Metrics definition

Connection Release Rate (CRR)

Since the attacker will never be able to successfully complete the authentication phase, the RRC connection will be closed with a rrcConnectionRelease message sent by the base station. This would never happen in a normal node, because the RRC connectivity remains stable, even in stand-by mode, unless the node were constantly performing handover to another base station.

$$CRR(x) = \frac{\#CR_X}{\triangle T} \tag{3.24}$$

where

$\mathbf{CR}_X$ = number of *Connection Request* messages on the current window

T = duration of the window

Average RRC Session Establishment (SMT)

A UE is considered to have established an RRC session once it is able to allocate a radio bearer to initiate the RRC authentication phase. This metric evaluates the frequency of RRC session established within a certain period of time. During the attack, all the attacking nodes will trigger a new RRC session establishment every time the *evolved-Node B* (eNB) reject the previous request due to incorrect challenge response or master key mismatch. Additionally, legitimate session establishments might be triggered on already established RRC sessions whenever the servicing network decides to reconfigure the link by reassigning a new bearer or changing

any additional parameter previously negotiated, affecting the effectiveness of this metric to distinguish between rogue and legitimate node behaviour.

$$ASE(x) = \frac{\sum SE_X}{n^2} \tag{3.25}$$

where

SE$_X$ = average *Session Establishment* duration for the sliding window x.

n = number of sessions established on the current window.

Session Success Rate (SR)

This metrics evaluates the number of successful RRC sessions established between each node and the serving eNB. Since the attacker nodes will not be able to complete any RRC session establishment, this metrics is expected to contribute positively to characterise the attack and reduce the uncertainty.

$$SSR(x) = \frac{\sum_0^x \#AA - \sum_0^x \#AF}{\sum_0^x \#CR} \tag{3.26}$$

where

AA = number of *Attach Accepted* messages sent on the current window.

AF = number of *Attach Failure* messages sent on the current window.

CR = total number of *Connection Request* messages registered on this window.

3.6 Summary

This chapter has defined the particularities of the detection algorithm presented on this thesis compatible with virtual jamming attacks in IEEE 802.11 wireless networks, and RRC signalling attacks in LTE cellular systems. The detection algorithm takes advantage of the automated BPA function created by F. Aparicio-Navarro et al. [66] to automatically estimate the probabilities of the three hypothesis evaluated on each scenario: the chances of having normal traffic, attack traffic or uncertainty due to the lack of enough evidence. The detection process is completed with the fuse of the source of evidence with D-S theory, producing a final outcome. To produce the evidence of the attack, five metrics have been presented for wireless communications: CRC, NAV, $\Delta Time$, DiffFSN and T. In a similar manner, three new metrics have been introduced for LTE systems: CRR, SMT and SR.

CHAPTER 4

Experimentation and result evaluation

4.1 Introduction

This chapter contains the analysis of results supporting the conclusions presented on this thesis, including a technical description of the two test-beds and all the scenarios recreated for collecting the datasets.

Section 4.2 defines the particularities of each test-bed and explains the design and implementation process to reproduce the selected *Denial-of-Service* (DoS) attacks. In a brief manner, the technical specifications are detailed for each network node, indicating its role on the attack and additional configuration parameters required to complete the execution.

The results displayed on this chapter are a small sample of the entire dataset generated by both test-beds. They are limited to the most representative cases for every scenario and the optimal sliding window size deducted for each technology. Each case is analysed in section 4.3, displaying a list of figures to reflect the evolution of the proposed metrics through all the phases of the attack.

The study and interpretation of the presented figures concludes this chapter, revealing the identification of patterns and node behaviours, and finally extracting conclusions from them.

4.2 Test-bed description

The first action of the experimental phase was the actual construction of the test-beds, which is a crucial part of this research project and main element for producing the dataset required to study both DoS attacks. As chapter 1 revealed, acquiring the necessary equipment for constructing an

Institute of Electrical and Electronics Engineers (IEEE) 802.11 network is an affordable and straight forward task, imposing the only challenge of identifying a *Wireless Network Interface Controller* (WNIC) chipset with a public source code for the driver controlling the wireless card.

However, deploying a cellular network demands a costly investment on equipment and represents a real legal challenge. The usage of radio spectrum is regulated by the *W*ireless Telegraphy Act 2006 [72], requiring a licensed allocation of the radio spectrum prior any emission over the frequencies used for 4^{th} *Generation of mobile communications* (4G) systems. Due to this impediment, the 4G test-bed was created using emulated hardware, which was interconnected with wired connections and signal attenuation devices to reproduce real urban propagation models.

The following paragraphs reveal the structure of each test-bed and present the list of technical equipment selected for their construction. Additional configuration parameters are also specified, including physical tampering and software-based amendments to reproduce the desired conditions on the scenarios defined on the following section 4.3. Finally, the role represented by each device on the attack is described, mentioning the software, scripts and standard Linux commands required to perform it.

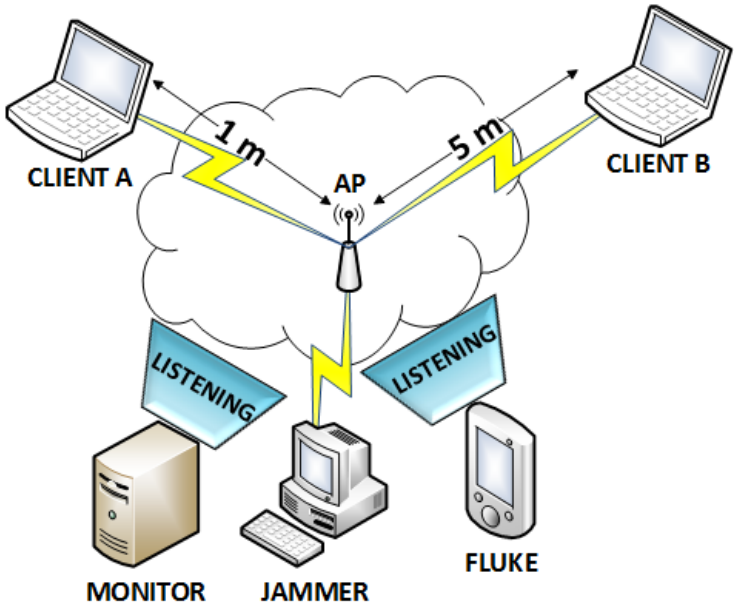


Fig. 4.1 IEEE 802.11 Test-bed Architecture

4.2.1 IEEE 802.11 Test-bed

This test-bed reproduces a standard configuration of an IEEE 802.11 network, with a variation on the number of mobile and static clients camping on it, and a single jamming node attacking at specific time intervals. There are four main stations: a jammer node, a monitor node, a Fluke Wireless Signal Analyser and client hosts; as described in figure 4.1.

Each station is configure as follows:

JAMMER

- This node runs on Linux Ubuntu 10.04 to meet the technical requirements and guarantee compatibility with the legacy *ar5k-driver* developed by R.Flöter et al. [73] for Atheros chipsets.
- The desktop computer was equipped with a WNIC using the Atheros 5100 chipset, which is fully compatible with the aforementioned driver.
- Manipulating the source code, the *Request-To-Send/Clear-To-Send* (RTS/CTS) mechanism was redefined to avoid listening to the channel when a collision occurs, and automatically set the *Network Allocation Vector* (NAV) duration to the maximum value.
- The modified version of the driver was compiled and loaded into the kernel, forcing an automated bound with the hardware during the OS booting process, replacing the official driver included in the kernel by default.

MONITOR

- This station has the only functionality of monitoring the communications and capturing all the network activity into a *Packet Capture* (PCAP) [74] file.
- The WNIC has the same Atheros chipset, which is configured in *MONITOR MODE* to listen to the channel.
- Using the *athstats* command, which is provided by the *ar5k-driver* driver to gather live statistics from the wireless interface card, the *Cyclic Redundancy Check* (CRC) errors are monitored through all the duration of the simulation.

FLUKE

- This device is a FLUKE Networks OptiView Series III Integrated Network Analyser, model OPVS3GIGW, including the Wireless LAN Adapter required to monitor wireless networks.

- Similar to the monitor station, this node captures all the traffic in a PCAP file for correlating the CRC error measurements with the Monitor node.

CLIENT

- The only function of this node is sending traffic through all the monitoring period.
- The traffic is generated artificially with the *IPERF* Linux command [75], which sends *User Datagram Protocol* (UDP) traffic at a constant rate.

The second well-behaved station was added to evaluate the detection performance with multiple clients located at different distances. The jammer station and both legitimate clients were interconnected using a single *Access Point* (AP) to cover the room where the test-bed was installed.

Monitoring the activity on the wireless network coverage area was conducted by two different nodes: a dedicated equipment designed for advanced network monitoring, named as FLUKE, which offers accuracy and reliable radio signal measurements; and a normal desktop workstation equipped with the same Atheros chipset and the modified version of the ar5k-driver, to guarantee the monitoring of all the CRC errors registered during the radio transmissions. The changes applied on the drivers are explained in Appendix B. Data from both monitoring stations was fused into a single PCAP file, using the timestamps to match the frames and merge the information captured on them.

4.2.2 LTE Emulation Test-bed

In contrast with *Wireless Fidelity* (WiFi) technologies, reproducing a LTE network within a research laboratory for experimental purposes is not a trivial task, due to the expensive equipment required for it and the legal implications of using public radio spectrum without the mandatory licenses. Researchers have been tackling this problem by establishing close bonds with the industry and collaborating with MNOs to share their testing installations for conducting research experiments. Additionally, there are several *Long Term Evolution* (LTE) software-based simulators in the market able to produce reliable results, such as LTE-Sim [76], NS3 [77] or OPNET [32], offering partial implementations of the LTE protocol and multiple path-loss models to imitate the characteristic of the radio channel.

This research project was initially focused on implementing the selected DoS attack within a simulated environment, aiming at verifying its feasibility beyond the theoretical approach, and evaluating its impact on the core-network components. Using OPNET Modeler Suite, it was possible to confirm the side effects that running the *Radio Resource Control* (RRC) signalling attack could inflict on the *Home Subscriber Server* (HSS). Figure 4.2 shows the

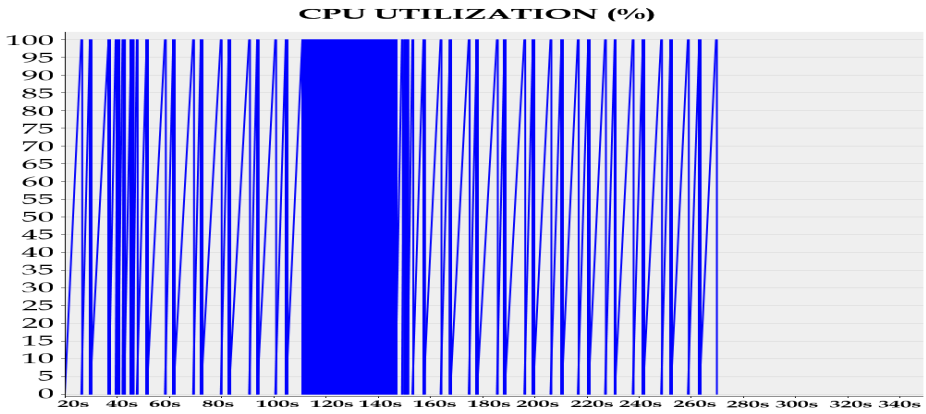


Fig. 4.2 CPU Utilisation Registered in the MME with 500 req/sec

Central Processing Unit (CPU) utilisation registered in the HSS, where the attack was able to saturate the resource in a short period of time. Once the attack was stopped after 4 minutes, the system quickly recovered back to its normal behaviour.

During this simulation, the attacker node was sending 500 RRC Connection Request messages per second using different *International Mobile Subscriber Identity* (IMSI) values, forcing the serving network to compute all the required cryptographic material to challenge the *User Equipment* (UE) and verifying its legitimacy. However, OPNET was not able to provide real traffic captures to be used when evaluating the proposed metrics to detect the attack. The LTE modules were in an early stage and there were not plans in the development pipeline to implement the additional traffic information for the lower layers in the protocol stack, which was the main interest of this research project.

Due to the limitations with OPNET, a physical test-bed was designed using hardware-based emulating equipment to run the required application-level services, and the core components composing a 4G deployment: Evolved Packet Core (EPC) entities, *Mobile Management Entity* (MME), *evolved-Node B* (eNB) and UE/s. The final architecture of the test-bed is displayed in figure 4.3.

APP TRAFFIC GENERATOR

- The network traffic was managed in a Lenovo ThinkCentre M73 Tiny Desktop PC, equipped with an Intel Core i3-4130T Processor (2.9GHz), 8 GB RAM and Windows 7 Pro 64 bits.
- This host was configured to run an FTP server with Microsoft IIS 6.0, allowing the UEs to perform file downloading via FTP to keep a continuous data flow through all the duration of the emulation session.

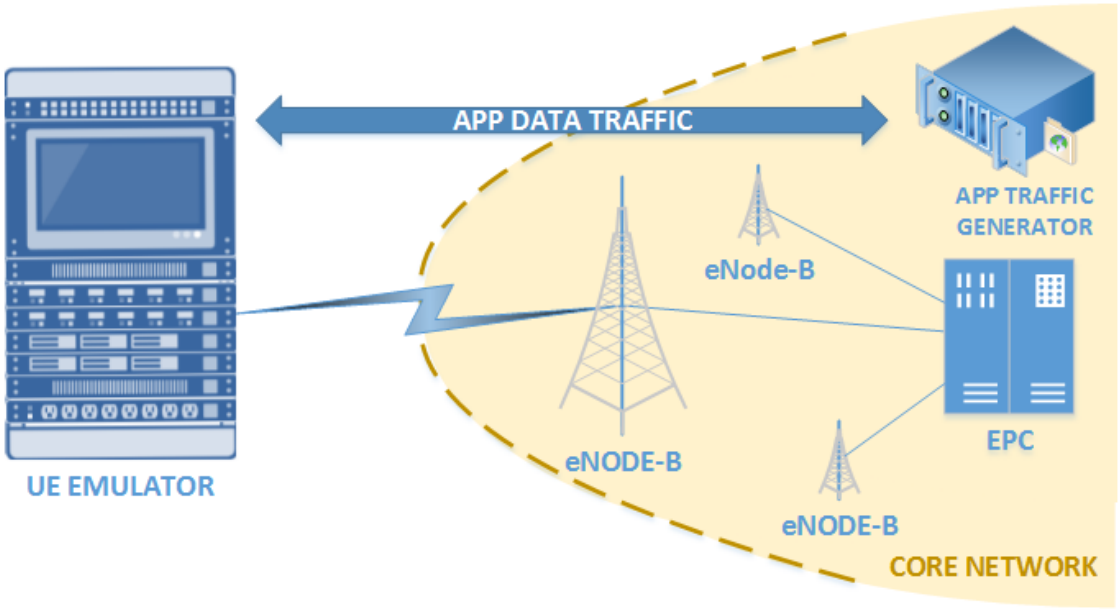


Fig. 4.3 LTE Test-bed Architecture

ENODE-B

- The RAN infrastructure was emulated using an LTE Enterprise Femtocell board, manufactured by Mindspeed with model number M84300, including a Transcend T3310 chipset for implementing all the standard LTE modulation schemes.
- The femtocell station was configured to have 3 sectors, requiring only one sector to create a single cell for camping all the UEs required for conducting the experiments.
- All the communications between the femtocell and the UE emulator were performed with wired connections and physical signal fading emulators, able to reproduce multiple radio path-loss schemes for signal attenuation. Free-space path-loss scheme was selected for this test-bed, making the UE emulator responsible for implementing the urban path-loss attenuation prediction on the registered radio measurements.

EVOLVED PACKET CORE (EPC)

- A single Aeroflex PXI 3000 modular platform was equipped with the Aeroflex LTE Base Station RF Measurements modules for providing the EPC capabilities to the test-bed.
- The equipment was configured to use FDD modulation for both downlink and uplink.
- All the UEs were registered in the HSS with the same master key, facilitating the implementation of the attack.

UE EMULATOR

- The UE emulation was managed in an Aeroflex E500 Network Tester, able to emulate the behaviour of up to 4000 UEs with the configuration used on this test-bed: 4 x Aeroflex TM500 modules interconnected to each other.
- The data traffic load was generated on the UE side using a Spirent C50 TestCenter, model number C50-KIT-04-START, with 4-port 10/1 Gbps Ethernet SFP able to manage a volume of up to 40 Gbps.
- The TM500 was configured to emulate different groups of malicious and legitimate UE nodes, as described in table 4.2.

4.3 Simulation scenarios

The simulation scenarios were designed to be compatible with the previously described test-beds, aiming at covering a wide variety of real-life use cases. The selected set of scenarios provides a rich dataset for each attack analysed, where edge cases are included to guarantee the best characterisation of the attacks. Minor variations are added on each scenario, by changing the number of active hosts, or their behaviour, to evaluate how efficient the proposed detection algorithm is when adapting to different network traffic patterns.

The following section 4.3.1 and 4.3.2 present each case studied and describe the required physical and software amendments to run each experiment. Explanatory graphics are included to represent the physical distribution of the equipment, as well as the main reasons for including every case on the dataset and the technical configuration applied on the active nodes.

4.3.1 IEEE 802.11 Scenario Definition

The proposed detection algorithm requires an initial training phase where it is fed with normal network traffic, as it is during this phase when the pattern for normality will be dynamically constructed. Due to this requirement, all the scenarios have been designed to meet the following three phases:

1. **INITIAL PHASE**
   The client stations are booted and the data transmissions are initiated among all the active nodes. This phase allows the detection algorithm to build a record of normal activity and create the baseline for all the metrics monitored.

2. **ATTACKING PHASE**
   The attacker station is enabled and the jamming frames are transferred through the

communication channel. The attacker is configured to cope with all the available resources and completely disrupt the communications of all the active clients throughout the duration of this phase.

3. **FINAL PHASE**
   The attacker is deactivated, leaving free the communication channel. This action will allow all the previously active nodes to proceed with their communications, and recovering the normal activity of the network.

Each phase has been set to a duration of 30 seconds with the aim of proving the resilience of the on-line detection algorithm for adapting to each phase and recover normality without reducing the detection rate. In all the scenarios, the monitor node and the fluke station are constantly sensing the channel and capturing all the activity on it.

Scenario	Client Nodes	Distance	RTS/CTS	IP Transport
1	1 x Static node	1m	No	UDP
2	1 x Static node	1m	No	UDP
	1 x Static node	5m	No	UDP
3	1 x Mobile node	-	No	UDP
4	2 x Mobile node	-	No	UDP
5	1 x Static node	5m	No	UDP
	1 x Mobile node	-	No	UDP
6	1 x Static node	1m	No	UDP
	1 x Mobile node	-	No	UDP
7	1 x Static node	1m	Yes	UDP
8	1 x Static node	1m	Yes	UDP
	1 x Static node	5m	No	UDP
9	1 x Static node	1m	Yes	UDP
	1 x Static node	5m	Yes	UDP
10	1 x Static node	1m	No	UDP
	1 x Static node	5m	Yes	UDP
11	1 x Static node	1m	No	TCP
12	1 x Static node	5m	No	TCP

Table 4.1 IEEE 802.11 Scenario Properties

The definition of each scenario takes into consideration the characteristic of the IEEE 802.11 standard and how the communication channel may be affected due to external factors. The client stations are considered to be in a static mode whenever there is no movement through all the duration of the experiments. In consequence, a client is considered a mobile node if it is in constant movement while the experiment is being conducted. The movement does follow a random direction and variable speed, reproducing a normal situation in real life.

Furthermore, two different distances are considered when placing the static nodes on each experiment: a short distance equal to 1m, and a long distance, which increases the separation by 5 times. The distance indicates how far the nodes are from the serving AP. This value is directly linked with the higher throughput a node can reach, due to the characteristics of the radio channel and the higher probability of suffering collisions when sensing the channel.

The last variable to take into account is the activation of the RTS/CTS mechanism, which forces the client node to listen the communication channel in search of any RTS and/or CTS control frames, respecting the channel availability dictated by other node's activity in the network. This mechanism can be manually activated/deactivated on each node independently of the role played on the experiment (attacker or client).

Table 4.1 provides a summary of all the evaluated scenarios, the number of active client nodes and the partial/total utilisation of the RTS/CTS mechanism for the nodes involved in the experiment.

The final two scenarios, scenario 11 and 12, evaluate the effects of the virtual jamming attack when the application traffic is encapsulated in *Transmission Control Protocol* (TCP) packages [78], instead of UDP datagrams [79]. TCP transport layer requires of a successful three-way handshake completion for establishing a TCP connection, making this communications more vulnerable [80] from suffering the side effects of the DoS attack.

Scenario 1

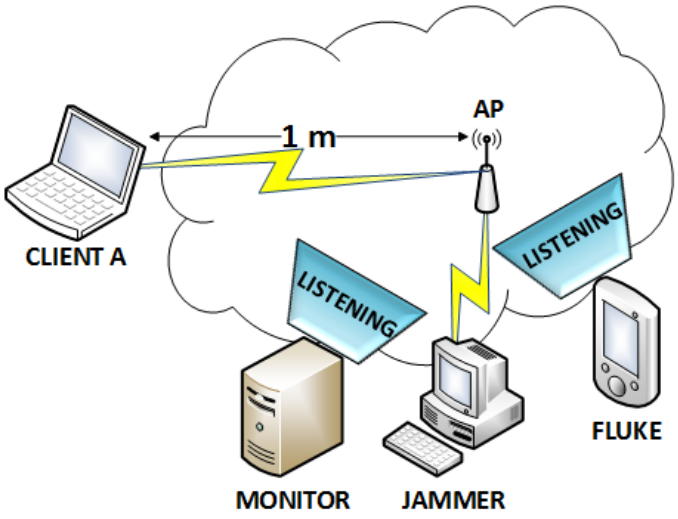


Fig. 4.4 IEEE 802.11 Attack - Test-bed for Scenario 1

This scenario reproduces a single client station camping the WiFi network on a fixed location close to the AP, with no mobility through all the duration of this experiment. There is

an inactive attacker node, which is temporary activated during the attacking phase, where the node jams the communication channel uninterruptedly.

Although this scenario only includes a potential victim node, Client A, the jamming node will manage to interrupt the communications not only to the active client, but also to any potential node attempting to attach to the AP while the attacking phase is active.

Scenario 2

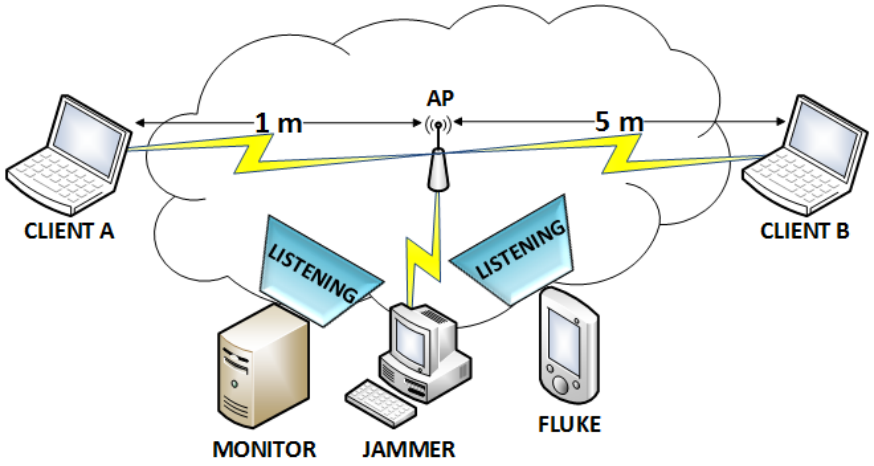


Fig. 4.5 IEEE 802.11 Attack - Test-bed for Scenario 2

In this scenario, a second client station is placed within the same Wi-Fi coverage area, increasing the distance within client and AP. During the attacking phase, both client stations are sending network traffic to the AP.

The attacker begins to jam the communication channel as soon as the attacking phase starts, provoking collisions on the radio channel whenever there is an on-going active transmission from/to the legitimate client nodes.

Scenario 3

Mobility is added into this scenario, using a single mobile node roaming around the AP coverage area while sending network traffic to the AP. The addition of mobility eliminates the stability on all the radio parameters of the WNIC, forcing the detection algorithm to dynamically evolve the normality pattern to consider this new variable.

It is noteworthy mentioning the direct effect of adding mobility on the metrics used for detecting the attack, having a less stable throughput through all the duration of the session, as well as a potential increase of CRC errors due to higher number of radio signal reflections affecting the radio bearer.

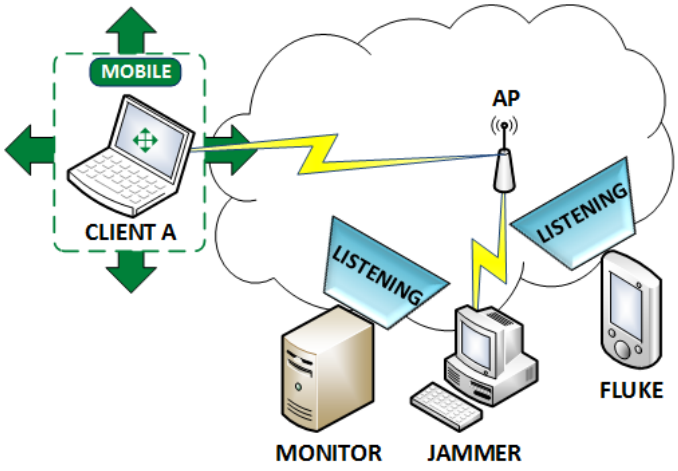


Fig. 4.6 IEEE 802.11 Attack - Test-bed for Scenario 3

Scenario 4

A second mobile node is added to the coverage area on this scenario, moving independently from each other across the room while following a random direction. Both nodes remains active through all the session, emitting data traffic in an endless loop. As a result of having two mobile nodes in constant data emission, the level of radio interferences increases with respect to Scenario 3, having higher probabilities of CRC errors.

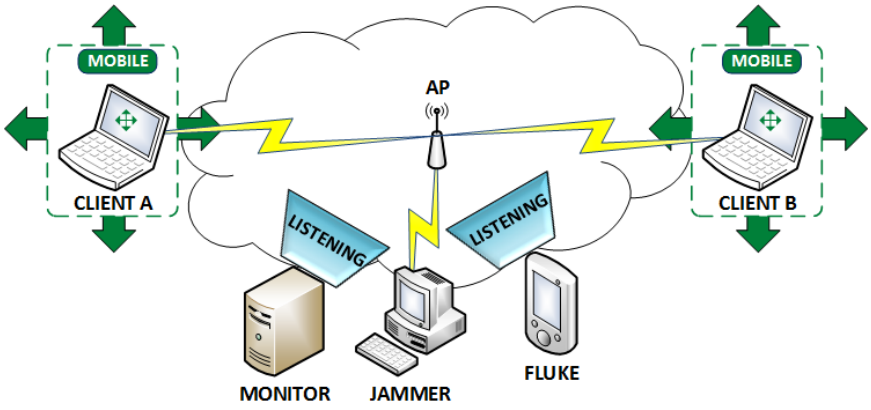


Fig. 4.7 IEEE 802.11 Attack - Test-bed for Scenario 4

Whenever the number of attached nodes is greater than one, the chances of suffering a higher number of collisions increases due to the well-known hidden node problem [81]. This phenomenon is specially harmful on this scenario, as the CTS/RTS mechanism is not enabled in any of the active clients, increasing the chances of simultaneous emissions from nodes located within the AP coverage area while being out of range from each other. This problem could lead

the detection algorithm to misclassifying some of the frames emitted by legitimate nodes as malicious, increasing the number of false alarms.

Other side effect to be considered is the longer waiting times imposed to the legitimate nodes when accessing the radio channel, as the number of active stations competing for the same communication channel has increased, having a direct impact in some of the metrics used by the detection algorithm, such as the NAV and Δ Time.

Scenario 5

Mobility remains active for one of the nodes on this scenario, placing the second node in a fixed position within a long distance from the AP. The fixed node act as intended actor for producing the hidden node problem whenever the mobile node exits its coverage range, as both nodes have been configured to continuously transmitting data through all the duration of the monitoring session.

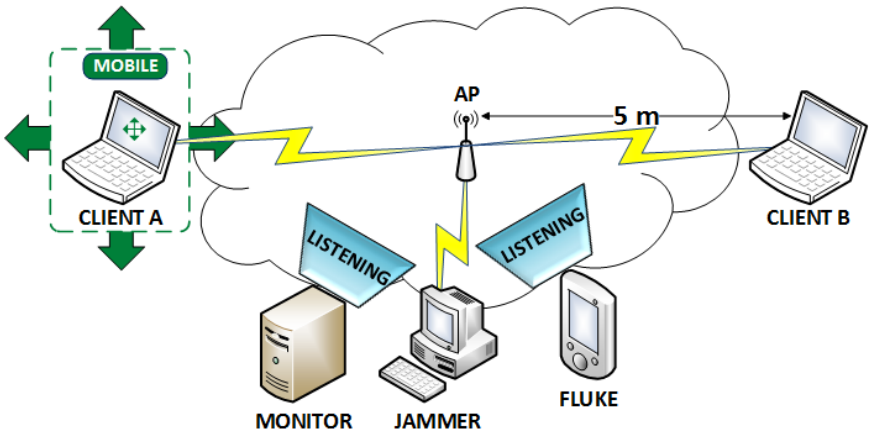


Fig. 4.8 IEEE 802.11 Attack - Test-bed for Scenario 5

Following the same reasoning described in the previous Scenario 4, a higher number of CRC errors are expected with a potential increase in the number of false alarms.

Scenario 6

This scenario reproduces the same conditions as Scenario 5, reducing the distance between the AP and the fixed node by 3 times as it is represented in figure4.9.

The probabilities of suffering from the hidden node problem are reduced considerably with regard to Scenario 5, although the threat remains active while having 2 active nodes and no RTS/CTS mechanism in place.

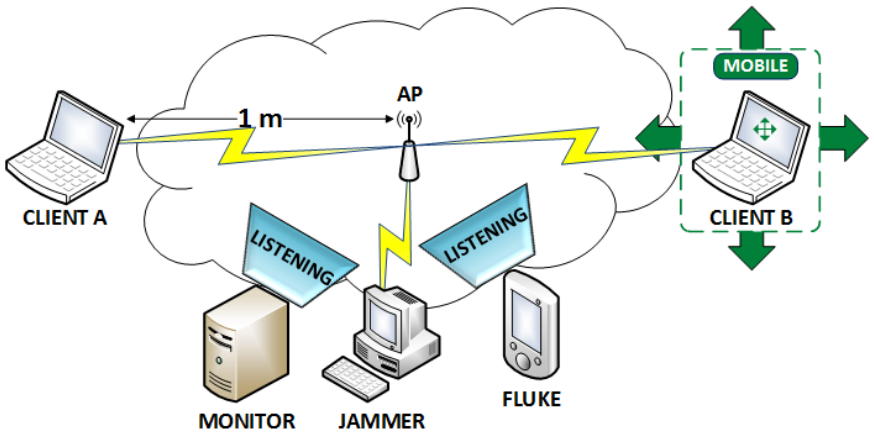


Fig. 4.9 IEEE 802.11 Attack - Test-bed for Scenario 6

Scenario 7

Introducing a new variable to the scenario, the RTS/CTS mechanism is enabled in a static node, Client A, which is placed within a short distance from the AP. Since there is only one active node in the wireless network, enabling the RTS/CTS mechanism will offer no benefit, as it only causes additional frame transmissions without being required. Looking at the similarities

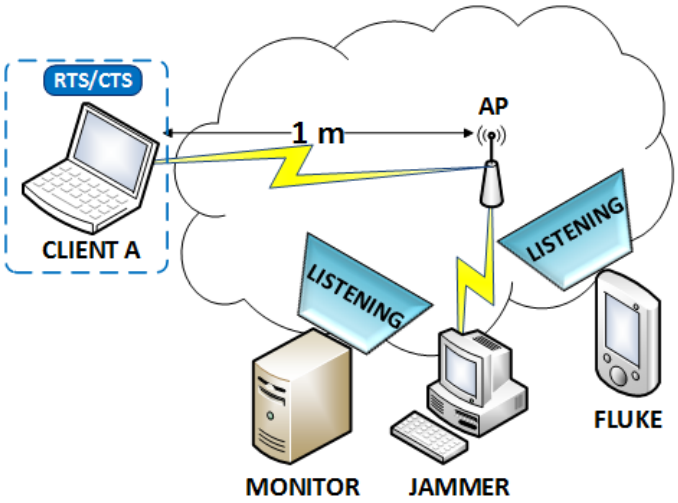


Fig. 4.10 IEEE 802.11 Attack - Test-bed for Scenario 7

between Scenario 1 and this scenario, which is depicted in figure 4.10, the detection algorithm is expected to provide similar results. The only metric expected to be affected by the additional transmission delays inflicted by the RTS/CTS mechanism, and the increase of the number of frames transmitted, is the Δ Time.

Scenario 8

In a similar manner to Scenario 2, two static nodes named as Clients A and Client B are placed within the same coverage area at a short and a long distance from the AP, respectively. Only Client A, which is the closest node to the AP, has the RTS/CTS mechanism active. Whenever a RTS/CTS frame is received in the AP, it will be broadcast to Client B, reducing the potential collisions and CRC errors.

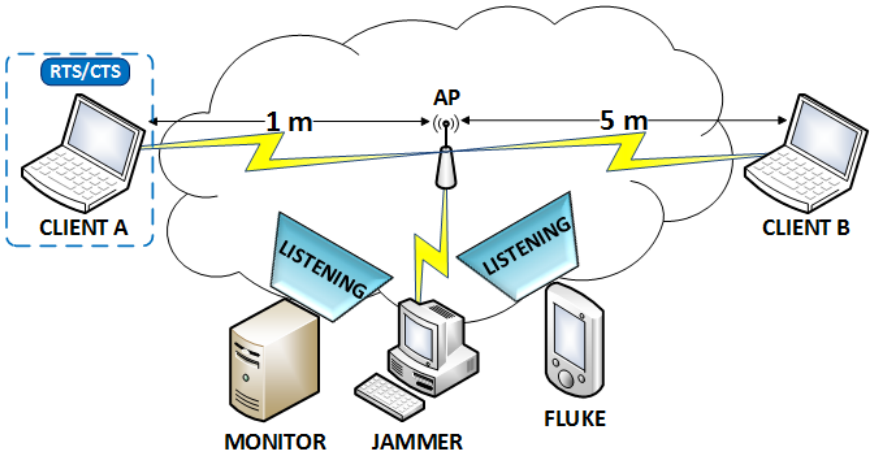


Fig. 4.11 IEEE 802.11 Attack - Test-bed for Scenario 8

However, Client B has the potential to provoke collisions, as no RTS/CTS control messages will be preceding/concluding its data frame transmissions.

Scenario 9

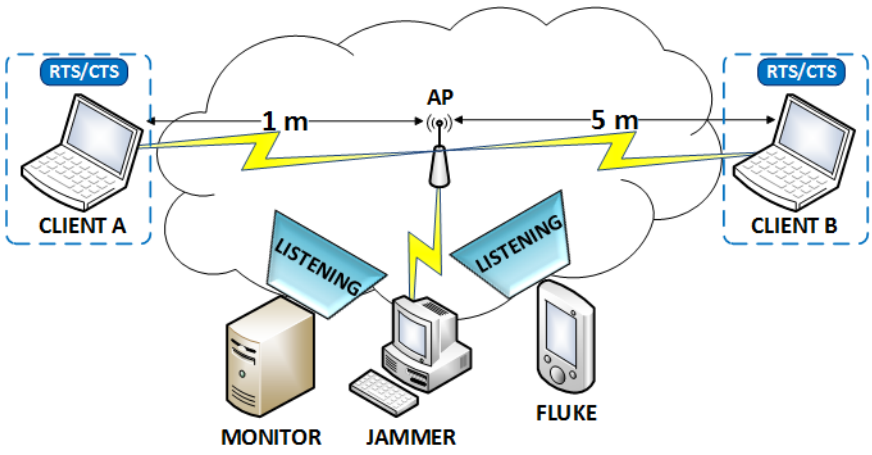


Fig. 4.12 IEEE 802.11 Attack - Test-bed for Scenario 9

Scenario 9 extends the conditions described in Scenario 8, to enable the RTS/CTS mechanism on Client B, the fixed node located at the furthest distance from the AP.

Reduced number of collisions are expected, due to the lack of mobility in both legitimate nodes and the additional safeguard measurement against the hidden node problem provided by the RTS/CTS mechanism.

Scenario 10

The last scenario using UDP as transport protocol is Scenario 10. It reproduces the conditions of Scenario 8, when only the static node located within a long distance from the AP has the RTS/CTS mechanism activated. Protecting this node will minimise the probabilities of suffering additional collisions in the communication channel.

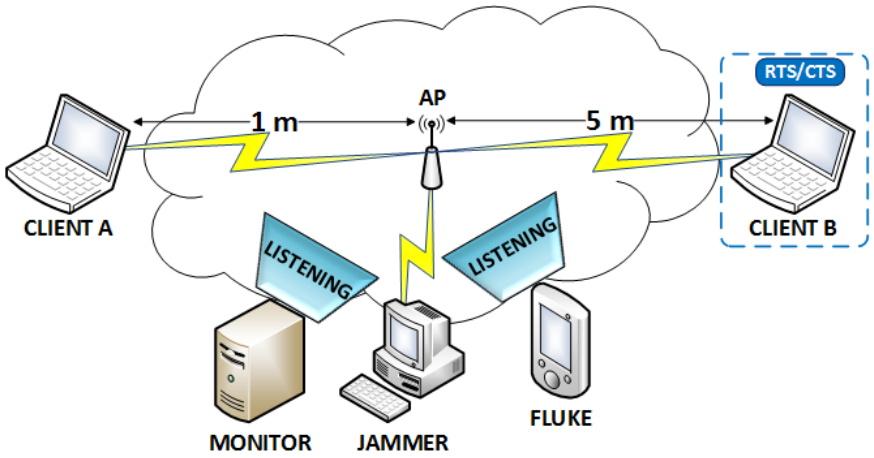


Fig. 4.13 IEEE 802.11 Attack - Test-bed for Scenario 10

Scenario 11

A single node is camping the WiFi network, sending TCP traffic to the AP, which is located within a short distance. The test-bed reproduces the same topology as in Scenario 1, modifying the network transport protocol used to transmit the data. This change does not affect neither the status of the lower layers in the protocol stack, physical and data link layer, nor the metrics computed from the information gathered from these two layers.

However, the data throughput might be affected due to the additional data exchange required for establishing a TCP session using the 3-way handshake [78].

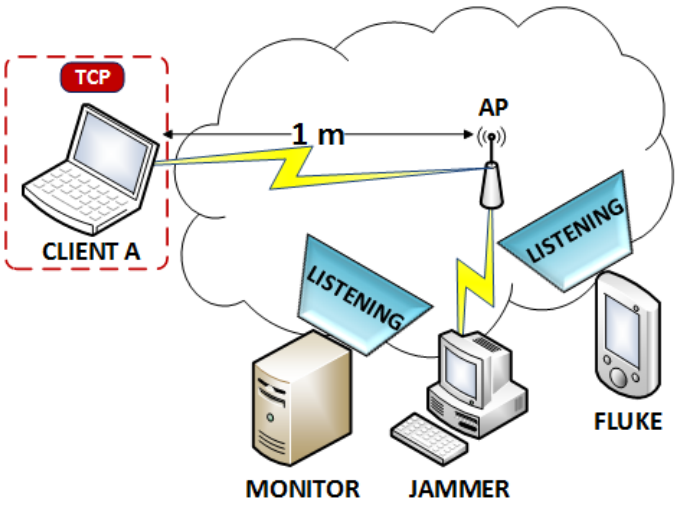


Fig. 4.14 IEEE 802.11 Attack - Test-bed for Scenario 11

Scenario 12

The last scenario, Scenario 12, evaluates the same conditions introduce in Scenario 11, repositioning the fixed node into a longer distance from the AP. The increase on the distance between

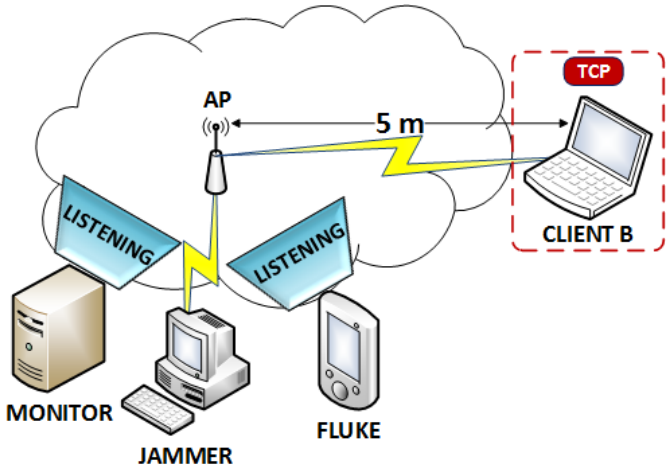


Fig. 4.15 IEEE 802.11 Attack - Test-bed for Scenario 12

the AP and the wireless node inflicts a variation in the radio signal strength on the physical layer, affecting the maximum data throughput reachable during the transmission. In particular, this scenario helps to understand how the establishment of a TCP communication session and management of the connection aliveness could increase/reduce the effectiveness of the DoS attack.

4.3.2 LTE Scenario Definition

The complexity of the design proposed for the LTE scenarios is a reduced representation of a commercial deployment, since the test-bed used is mainly composed with an LTE emulated eNB connected to an emulated LTE core network. Due to the method selected for implementing the RRC signalling attack, it is possible to identify two types of UE nodes: legitimate UEs, using a valid master key (K) value and registered in the HSS as active subscribers; and rogue UEs, which are also registered in the HSS and have been configured with an incorrect K value, to force a failure during the establishment of a RRC session.

In a real-life attack, the attacker would perform exactly the same actions, as the only information under its control would be the IMSI value of legimitate UEs, but it would not be able to compromise the private K associated to every mobile subscriber.

Since the aim of a malicious user is to disrupt the service in the most efficient manner, the attacker role was configured to be composed by multiple sets of rogue UEs acting as a single attacker node. Only by having multiple rogue UEs attempting to establish RRC sessions in parallel, it is possible to reproduce the equivalent network traffic volume produced by a single attacking UE targeting a commercial LTE cell.

The ratio between legitimate and rogue nodes has been modified across the three scenarios, as described in table 4.2 offering a wider vision of the impact on core equipment when the rogue traffic load is equal and higher than the traffic generated by the legitimate UEs.

In contrast with the wireless scenario definition introduced in section 4.3.1, the duration of initial and attacking phases is set to 30 seconds for the Scenario 1, and 5 minutes for Scenario 2 and Scenario 3; whereas the duration of the final phase varies on each scenario. Moreover, the time allocated to the initial and attacking phases includes the time required for initiating the legitimate and malicious UEs, having a gradual increase in the cellular network traffic received at the eNB.

Scenario	Legitimate UEs	Rogue UEs	Initial/Attack Phase	Final Phase	Total Duration
1	200	200	30 sec	95 sec	2 min 35 sec
2	50	450	300 sec	221 sec	13 min 41 sec
3	200	200	300 sec	431 sec	17 min 11 sec

Table 4.2 LTE Scenario properties

The attack duration represented in table 4.2 for the initial and attack phases is the total duration of each phase individually, including the time required for booting all the UE nodes participating in the emulation as legitimate and rogue UEs, respectively.

Scenario 1

This scenario is composed by an equal number of legitimate and rogue nodes, located within the same cell and attached to the same eNB. The aim of this scenario is to prove how effective

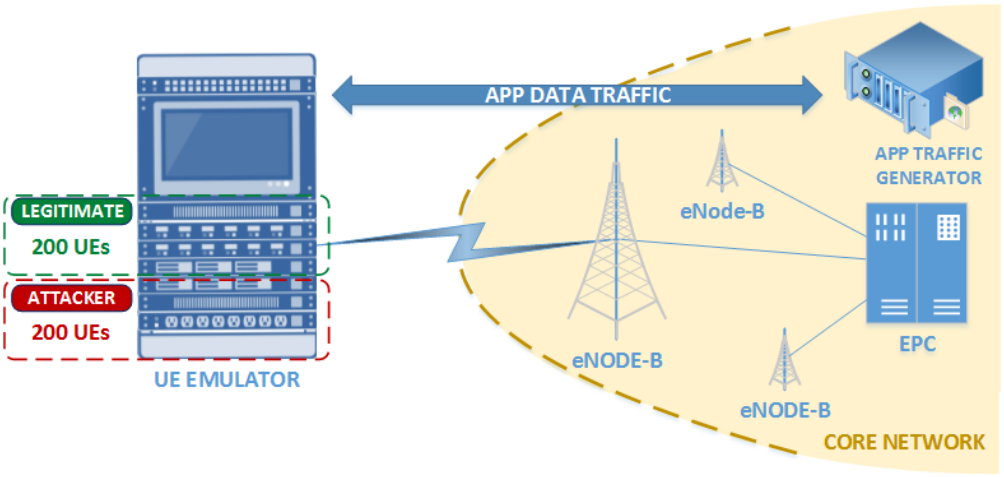


Fig. 4.16 LTE Attack - Test-bed for Scenario 1

the detection algorithm is when the network traffic load generated by the attacker and the legitimate UEs has a similar magnitude. However, it is expected to register a higher number of messages exchanged between the rogue nodes and the eNB, as the legitimate UEs only require to establish an RRC session once. Meanwhile, the rogue UEs will continuously attempt to establish new RRC sessions, triggering the exchange of multiple control frames. The duration of the monitoring session has been reduced to less than 3 minutes to preserve the ratio of control/data frames transmitted by legitimate and rogue UEs through all its duration.

Scenario 2

Using a higher proportion of rogue nodes, this scenario emulates the worse case when the rogue network traffic overpasses the legitimate traffic through all the attacking period. The aim of this case is to study the effectiveness of the detection algorithm constructing the normality pattern when it is fed with a reduced number of legitimate samples. Due to the fact that the number of attacker UEs is 9 times bigger than the legitimate nodes, this scenario presents a real challenge for the detection mechanism.

Nonetheless, the duration of the emulation has been extended to guarantee enough iterations for the normal buffer to construct the normality pattern, and measuring the recovery time required until the detection rate becomes stable.

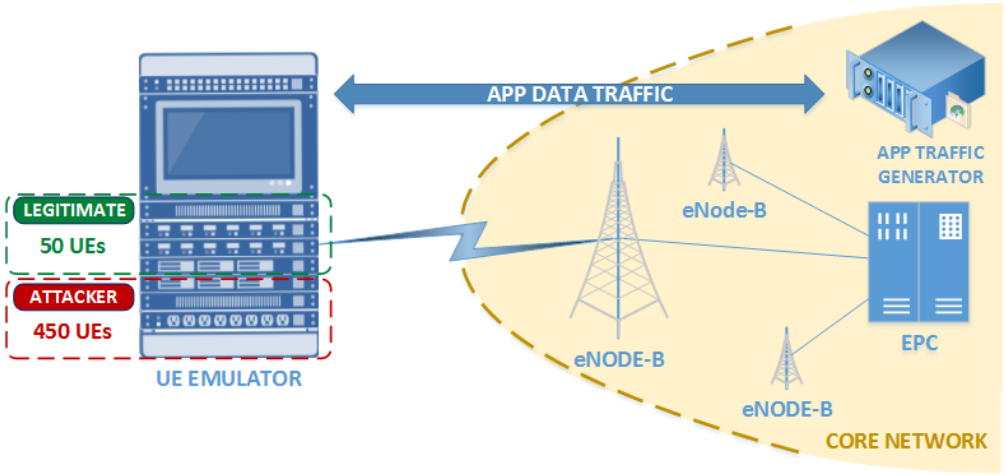


Fig. 4.17 LTE Attack - Test-bed for Scenario 2

Scenario 3

Although this case has the same legitimate/rogue nodes ratio as described in figure 4.16, Scenario 3 extends the emulation time for a longer period. Using a wider emulation duration, the detection algorithm has additional time to recover normality once the attack has finished, allowing a more accurate assessment of the detection efficiency.

During a longer monitoring session, it is also possible to challenge the detection algorithm during the attacking phase, as the traffic load generated by legitimate and rogue UEs will evolve during the five-minutes duration of this phase. At the beginning of the attacking phase, some legitimate UEs are expected to produce similar control traffic loads as the rogue UEs, which will be gradually enabled during the first 20 seconds. Once all the rogue nodes are active, their traffic pattern will remain the same, while the legitimate UEs are expected to register higher data traffic rates and minimal control traffic, to keep the RRC session active.

4.4 Results

The last section of this chapter contains a summary of the results collected for each technology, using the test-bed described on section 4.2 to run a set of scenarios and collecting network traffic from each node. The network traffic composes the dataset used for computing the proposed metrics, and proceed with the evaluation of their effectiveness when being used for detecting the DoS attacks targeted on this thesis.

The evaluation of the detection performance is conducted using different performance indicators, which are introduced in Section 4.4.1, allowing a better understanding of the results obtained on each scenario. The last requirement before proceeding with the detection of the

attack on each experiments is the definition of the optimal *Sliding Window* (SW) size, as it has to be tailored to the particular attack studied for an optimal detection performance. The discussion and final establishment of the optimal size for the SW is conducted in Section 4.4.2.

Section 4.4.3 provides a summary of the most suitable set of metrics to detect the virtual jamming attack across all the scenarios, highlighting other cases where the detection rate remains within an acceptable ratio while adding modifications on the set of metrics used on the detection.

In section 4.4.4, the results for the LTE signalling attack are studied following the same approach applied for IEEE 802.11 and revealing the most suitable set of metrics for each scenario presented. In contrast with the previous section, where a wide range of detection performance rates are presented depending of the metrics evaluated on each analysis, the results obtained for the LTE experiments have been proven an overall high effectiveness for identifying the attack no matter the metric combination used.

4.4.1 Evaluating the Detection Performance

The data collected during the execution of the test cases was processed off-line for extracting representative data and automate the calculation of each metric evaluated. Using the information extracted from each frame, every metric was computed, and automated beliefs were assigned for the three hypothesis: normal, attack or uncertainty; using the automated *Basic Probability Assignment* (BPA) function introduced by K. Kyriakopoulos et al [69]. Using the computed beliefs, a final decision is made for each frame to classify it as attack or not attack by fusing the beliefs with D-S theory as indicated in the previous chapter 3.

Analysing the performance of the detection algorithm is a challenging process, requiring the study of several parameters to better understand how effective the algorithm performs when identifying the attack. Using multiple performance indicators, it is possible to avoid constructing the analysis of the results with incomplete and/or misleading information.

This thesis evaluates the usual parameters applied for assessing result performance in pattern recognition, data mining techniques and the statistical analysis of binary classifications [82], as the final target of the detection algorithm is answering the attack/no attack hypothesis for each frame.

The first step to evaluate the performance is the definition of the classification for all the predictions of the algorithm into 4 categories:

TP: A *True Positive* event occurs whenever an attacker's frame is correctly identified by the detection algorithm as malicious.

FP: A *False Positive* event indicates that the detection algorithm has misclassified a normal frame as malicious, also named as Type-I error.

TN: A *True Negative* event is a successful classification of a normal frame by the detection algorithm.

FN: A *False Negative* event is also called Type-II error, as it means that a malicious frame has been missed by the detection algorithm, and incorrectly marked as normal.

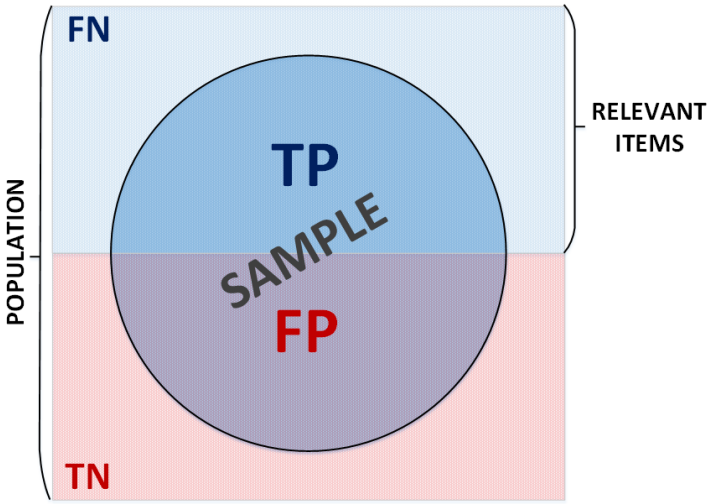


Fig. 4.18 Graphical Representation of the Detection Performance Indicators

In the following figure 4.18, the population is represented by the final decision computed by the algorithm for each frame registered in an specific scenario. The relevant items are the values within the populations that falls into the 'attack' category, no matter if they have been successfully identified (TP) or misclassified by the algorithm (FN). The sample or selection is composed by the results of the algorithm, with all the frames classified as 'attack', including both the TP and FP cases.

Using the definitions previously described, the following performance indicators can be defined for evaluating the detection algorithm [82, 70]: *Detection Rate* (DR), *False Positive Rate* (FPR) and *False Negative Rate* (FNR). The DR, also known as *True Positive Rate* (TPR), Recall or Sensitivity, indicates the proportion of malicious frames detected in comparison with the total number of frames emitted by the attacker. This parameter offers a clear indication of how efficient the detection algorithm is. However, this value is not able to provide a fair assessment of the detection performance by itself and could lead to an error when analysed individually, since it does not take into account the negative effects of misclassifying malicious

frames as normal (FN), or the opposite case when a false alarm is raised (TN) as result of applying the detection algorithm.

$$DR = \frac{TP}{TP+FN} \tag{4.1}$$

$$FPR = \frac{FP}{TotalFrames} = \frac{FP}{TP+FP+TN+FN} \tag{4.2}$$

$$FNR = \frac{FN}{TP+FN} \tag{4.3}$$

This information has a direct impact into the overall detection performance and must be taken into account when analysing the performance. Looking at the test evaluation in pattern recognition theory [82] and *Intrusion Detection System* (IDS) [83], it is possible to judge the performance in a more complete manner by evaluating: the *Overall Successful Rate* (OSR), also known as accuracy, which takes into account the correctly classified frames against the total population; the *Precision* (P), also known as the *Positive Predictive Value* (PPV), which evaluates the number of frames correctly classified malicious among the total of frames classified as malicious by the algorithm; and finally, the F_1-Score, also known as F-Score or F-measure, which is the harmonic mean of the DR and Precision, and evaluates the balance between these two parameters.

$$OSR = \frac{TP+TN}{TP+FP+TN+FN} \tag{4.4}$$

$$P = \frac{TP}{TP+FP} \tag{4.5}$$

$$F_1 - SCORE = \frac{2*P*DR}{P+DR} \tag{4.6}$$

In general, high values of the DR and F_1-Score indicates a good performance of the detection algorithm. However, it is important to remark that the OSR parameter might cause confusion and also lead to misinterpretation of the performance, since it assumes equal weight to both types of errors (FP and FN), and the successful frame classifications (TP and TN). This might cause the OSR to reach high values even when the DR is quite poor. Only the analysis of all the parameters described on this section as a group provides a correct interpretation of the results.

4.4.2 Sliding Window Size

The detection algorithm rely on a pre-defined SW size, which must be optimised and tailored for each technology to guarantee the highest efficiency on the detection rate. An initial analysis of the SW size was conducted on every experimental scenario, for both cellular and wireless

networks, covering multiple sizes within the range of 2 to 50 samples with 5 sample increments, and all the distinct permutations in metric combinations. This analysis produced 341 and 77 combinations for each WiFi and LTE scenario, respectively, composing a dataset with 4092 and 231 evaluations of the proposed algorithm. Figure 4.19 and figure 4.20 show the results of this analysis, displaying the average DR obtained when analysing the captured network traffic on each test case for every different SW size and metric combination evaluated.

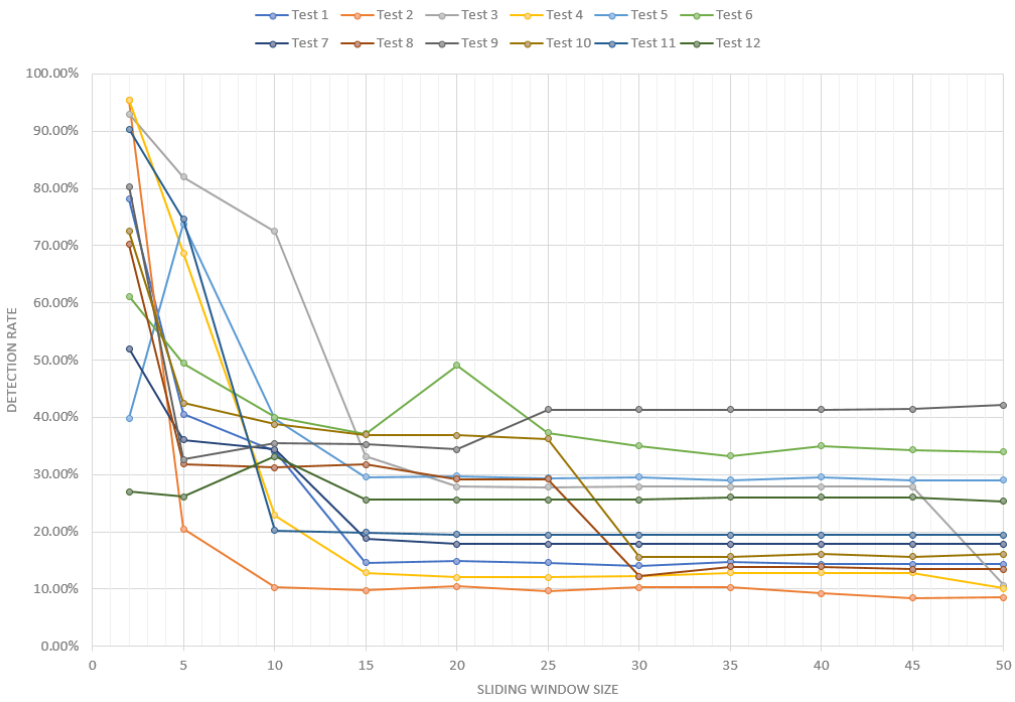


Fig. 4.19 IEEE 802.11 - Average Detection Rate based on Sliding Window Size

In general, the graphs show how the DR tends to stabilise for SW sizes equal or bigger than 20 samples, while the maximum DR is obtained for lower sampling groups of 2-5 items. However, using low sampling groups make the detection algorithm more vulnerable against peak values on the DR, reducing its adaptability to pattern changes in the network traffic flows. This is the reason for selecting the SW size with the highest DR right after the peak DR values registered for the smaller SW sizes.

Following the same approach, if all the results are aggregated for every scenario into a single graph, representing the average DR value grouped by SW size, a similar pattern is revealed with a stabilisation point when the size is equal or bigger than 30 samples, represented in the following figure 4.21 and figure 4.22.

Once all the cases have been grouped by the SW size, it is possible to identify that the SW size of 20 samples seems to be the most optimal for the IEEE 802.11 test-bed, with the peak

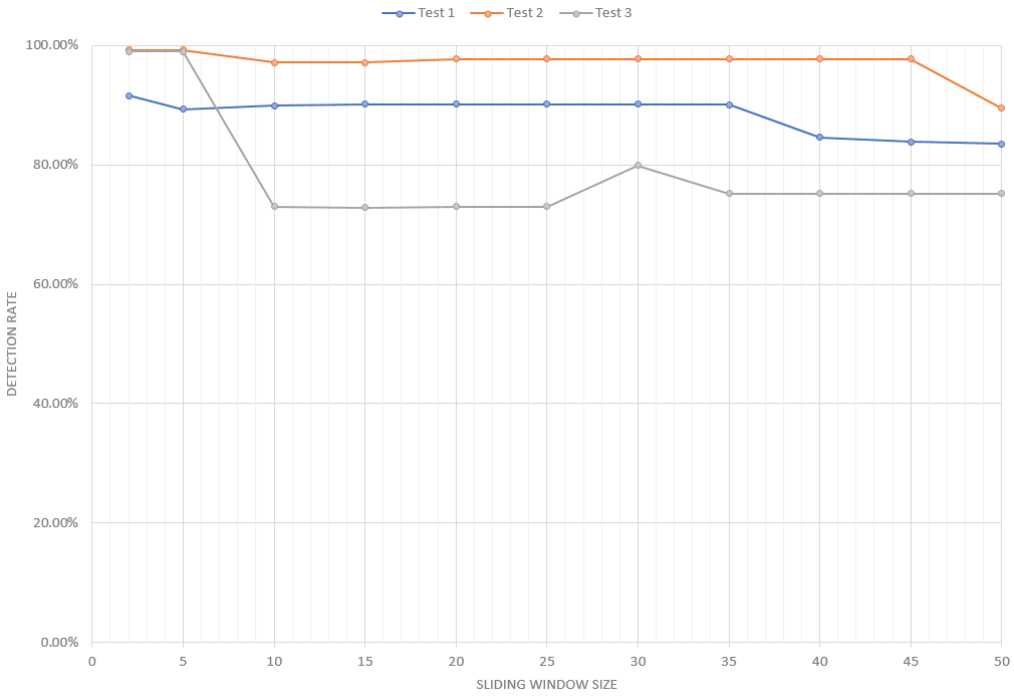


Fig. 4.20 LTE - Average Detection Rate based on Sliding Window Size

DR value once the algorithm has stabilised, having the lowest distance between the average and mean DR value. However, the optimum size for the LTE test-bed seems to be when the SW size is equal to 30 samples, as the graph represent a clear peak value of the DR after the algorithm has stabilised.

In order to make the final decision, it is necessary to take into account all the performance indicators described on section 4.4.1, as they help to reduce uncertainty and provide a more accurate picture of the detection performance. Figure 4.23 support the selection of 20 SW size as optimal value, where the average DR reaches its peak value of 25.63% while still having an average F_1-Score of 12.01%. Looking at the detection performance indicators for the LTE experiments, represented in figure 4.24, the SW size of 30 samples remains the most optimal with an average DR of 89.30% and F_1-Score of 89.66%.

Although in all the figures included on this section the SW size of 2 and 5 samples obtain a better DR and F_1-Score, they are not considered optimal for a live IDS,. This is due to the fact that having such a low size would make the system more vulnerable to peak values in the metrics monitored, which could occur as part of a natural evolution of the node behaviour over the time.

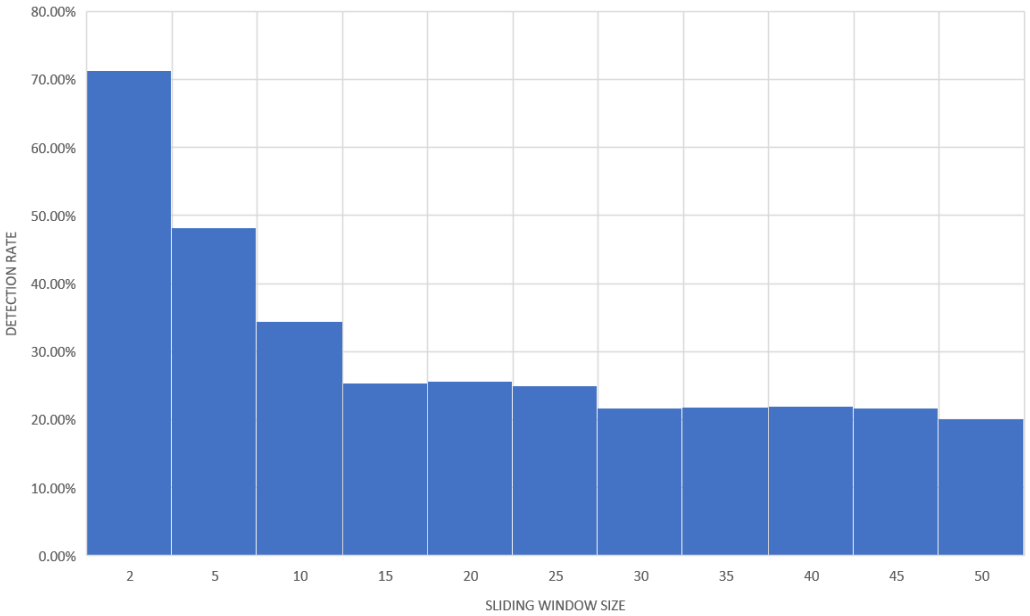


Fig. 4.21 IEEE 802.11 - Global Average Detection Rate based on Sliding Window Size

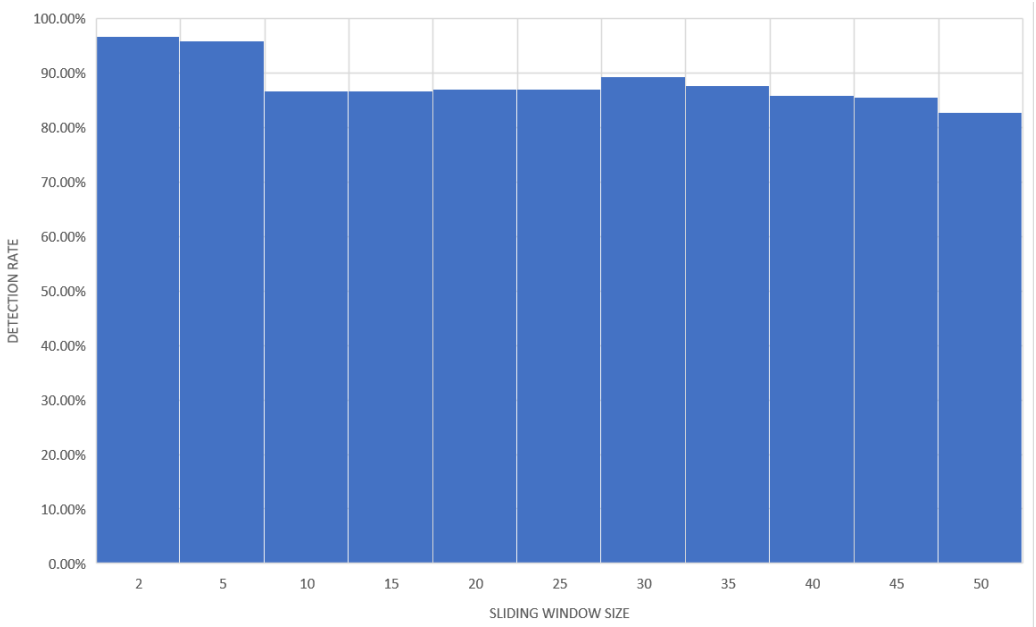


Fig. 4.22 LTE - Global Average Detection Rate based on Sliding Window Size

4.4.3 IEEE 802.11 Results

Finally, this section provides a summary of the results collected while analysing each scenario, showing the highest DR obtained on each case, and the most suitable metric combinations to

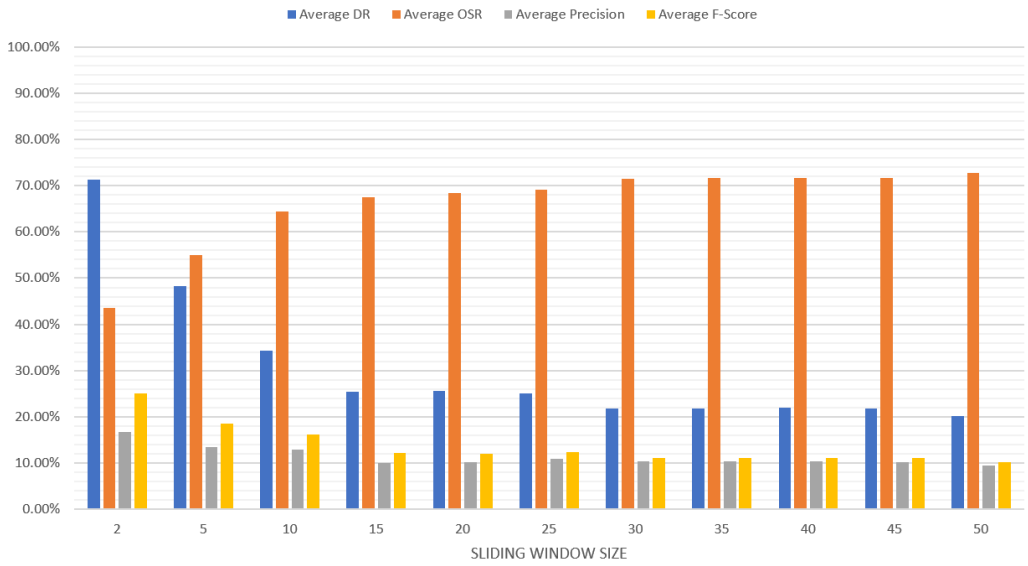


Fig. 4.23 IEEE 802.11 - Global Detection Performance

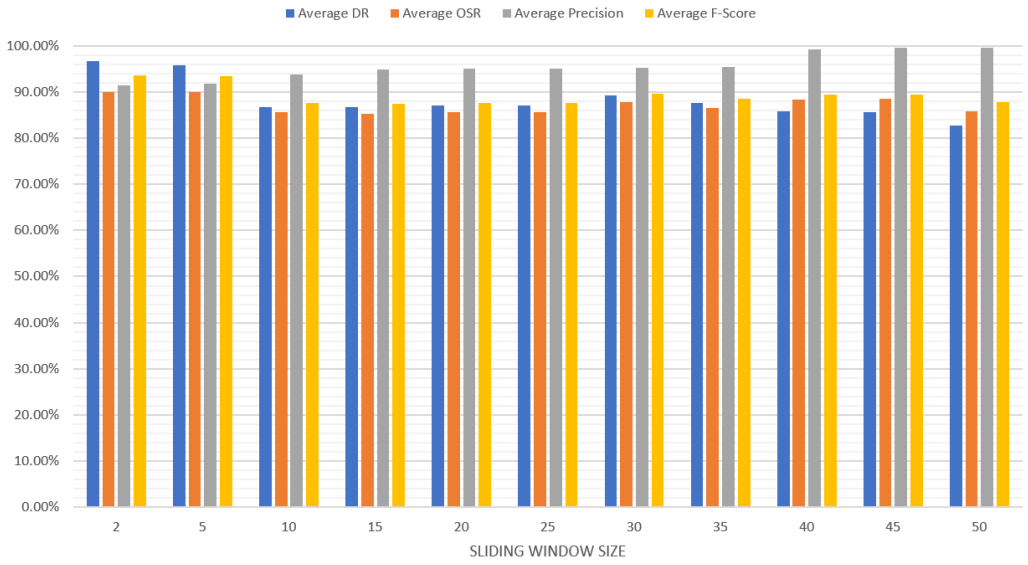


Fig. 4.24 LTE - Global Detection Performance

accurately detect the virtual jamming attack as part of the security mechanism implemented on an on-line IDS.

Nonetheless, the overall results for IEEE 802.11 networks can be summed up on table 4.3 with the individual analysis of the NAV metric, which provides the highest DR on all the scenarios using the optimal SW size. This table also provides a view of the magnitude of data

collected on each scenario, decomposing the total of frames captured into the basic performance indicators of FP, FN, TP and TN.

Scenario #	FP (%)	FN(%)	TP(%)	TN(%)	Total frames	DR(%)
1	0.11	0.00	25.16	74.73	143,814	100.00
2	7.93	0.00	17.53	74.54	112,895	100.00
3	0.10	0.00	22.91	76.99	143,558	100.00
4	2.98	0.00	5.05	91.97	130,692	100.00
5	2.62	0.00	12.47	84.90	139,622	100.00
6	2.18	0.00	3.81	94.01	140,810	100.00
7	1.73	0.00	26.64	71.63	115,059	100.00
8	21.58	0.00	18.35	60.07	143,483	100.00
9	34.70	0.00	9.10	56.19	130,892	100.00
10	12.90	0.00	13.22	73.88	110,867	100.00
11	4.53	0.00	12.24	83.23	204,262	100.00
12	5.72	0.00	12.49	81.79	145,494	100.00

Table 4.3 Summary of the detection performance for IEEE 802.11

This case is based on a single metric, the NAV metric, allowing the detection of the attack with a 100% accuracy on all the scenarios. The SW was configured with a size of 20 samples.

However, FP and FN ratios can be observed in most of the cases, being required a combination of metrics on the analysis for taking more reliable decisions not based in a single source of evidence. Using multiple metrics in the analysis provides robustness to the detection process in complex scenario where the uncertainty increases.

The following sections evaluate additional combinations of metrics and sliding sample window, studying the results obtained and indicating the advantages and/or disadvantages on each case. Further data collected during the experiments have been excluded from this chapter due to space restrictions, and can be found in Appendix A. The original scripts used for implementing the detection algorithm are also presented in Appendix B.

Scenario 1

The analysis of Scenario 1 reveals the most effective metric for detecting the WiFi DoS attack studied on this thesis: the NAV. Looking at the processed results displayed in table 4.4, the

individual analysis of the NAV metric provides the highest DR value, being able to identify the majority of malicious frames for this scenario with an OSR of ∼99.89% and F_1-Score of ∼99.78%.

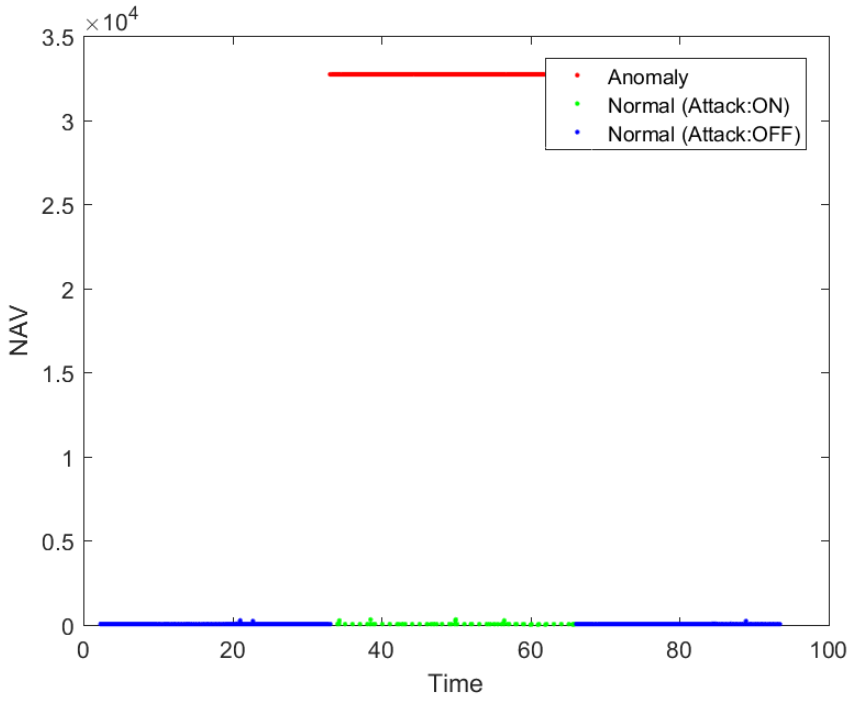


Fig. 4.25 Metric for IEEE802.11 Scenario 1 - NAV

Alternatively, the Δ Time metric has proven very effective on this scenario, registering a DR of 82.61% when used individually or as part of a set with the NAV metric. In both cases, the OSR, Precision and F_1-Score parameters registers the same value of ∼35.13%, ∼25.57% and ∼39.05% respectively, which is an acceptable performance for a commercial IDS.

On the contrary, the poorest performance is achieved when the CRC metric is evaluated individually, with a FNR rate of 100%, which indicates that all the malicious frames were incorrectly tagged as normal. The OSR indicates a ∼72.60% success rate due to the correctly classified normal frames (TN). This parameter might cause confusion due to the high value registered, unless the Precision and F_1-Score are also reviewed.

The OSR becomes more useful when analysing the other 14 metric combinations producing the same 0% DR, where a slightly higher OSR of ∼74.85% is appreciated, in comparison with the previously mentioned case. This difference is due to the error inflicted by the 2.24% FPR when the detection algorithm only uses the CRC metric, which has been reduced to 0% causing the proportional increase on the OSR.

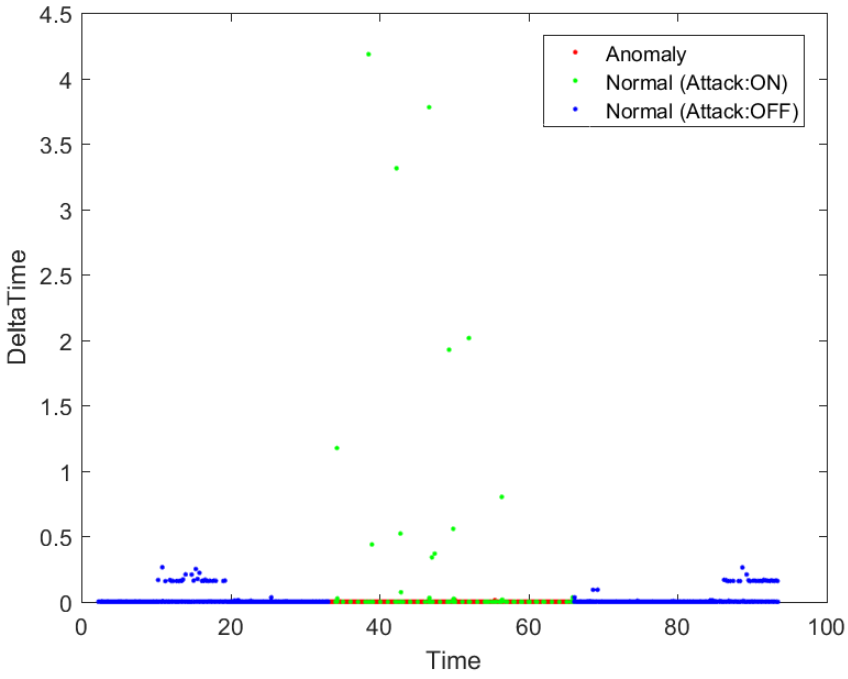


Fig. 4.26 Metric for IEEE802.11 Scenario 1 - Δ TIME

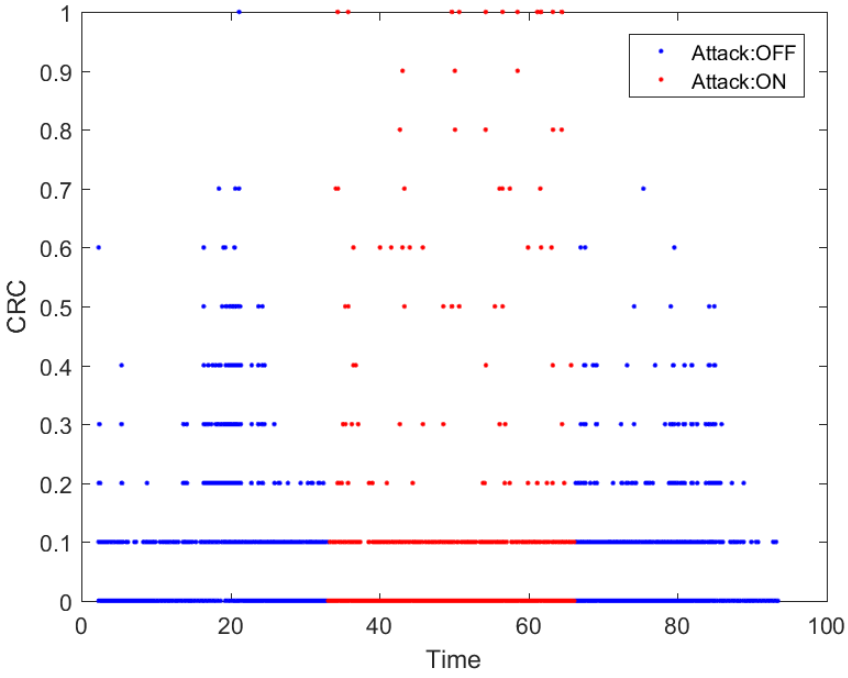


Fig. 4.27 Metric for IEEE802.11 Scenario 1 - CRC

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	0.113%	99.887%	99.551%	99.775%	NAV
82.613%	17.387%	60.494%	35.132%	25.569%	39.052%	$\Delta Time$
82.613%	17.387%	60.494%	35.132%	25.569%	39.052%	$\Delta Time, NAV$
69.544%	30.456%	17.281%	75.058%	50.307%	58.382%	$\Delta Time, T, NAV$
39.840%	60.160%	17.249%	67.617%	36.749%	38.232%	T, NAV
39.840%	60.160%	17.279%	67.588%	36.710%	38.211%	$\Delta Time, T$
39.818%	60.182%	17.249%	67.612%	36.736%	38.215%	T
1.183%	98.817%	27.695%	47.447%	1.063%	1.120%	DiffFSN
1.183%	98.817%	27.695%	47.447%	1.063%	1.120%	DiffFSN, NAV
1.045%	98.955%	23.877%	51.230%	1.089%	1.066%	$\Delta Time, DiffFSN$
1.045%	98.955%	23.877%	51.230%	1.089%	1.066%	$\Delta Time, DiffFSN, NAV$
0.923%	99.077%	10.358%	64.719%	2.193%	1.299%	T, DiffFSN, NAV
0.923%	99.077%	17.183%	57.894%	1.334%	1.091%	$\Delta Time, T, DiffFSN$
0.923%	99.077%	17.183%	57.894%	1.334%	1.091%	$\Delta Time, T, DiffFSN, NAV$
0.509%	99.491%	10.356%	64.617%	1.220%	0.718%	T,DiffFSN
0.066%	99.934%	0.097%	74.764%	14.634%	0.132%	$\Delta Time, T, DiffFSN, NAV, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	T, CRC
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, T, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	DiffFSN, CRC
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, DiffFSN, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	T, DiffFSN, CRC
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, T, DiffFSN, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	NAV, CRC
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, NAV, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	T, NAV, CRC
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, T, NAV, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	DiffFSN, NAV, CRC
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	$\Delta Time, DiffFSN, NAV, CRC$
0.000%	100.000%	0.000%	74.845%	0.000%	0.000%	T, DiffFSN, NAV, CRC
0.000%	100.000%	2.240%	72.605%	0.000%	0.000%	CRC

Table 4.4 Results for IEEE 802.11 Scenario 1 with SW=20

If the individual values registered for the NAV and Δ Time are observed on Scenario 1, represented in figure 4.25 and figure 4.26 respectively, a clear pattern arises for differentiating normal and malicious frames. Looking at figure 4.27, where the values registered for the CRC metric are plotted, the difficulty of discerning between anomaly and normal behaviour becomes more obvious.

Scenario 2

In Scenario 2, the NAV metric registers a slightly lower F_1-Score of ∼81.55% in comparison with the previous Scenario, followed by the results provided by the Δ Time metric, with a very close ∼98.55% DR but less than half of the OSR and F_1-Score. Surprisingly, the combination of these two metrics does not improve the results produced when using the Δ Time metric individually, having exactly the same value on all the performance indicators.

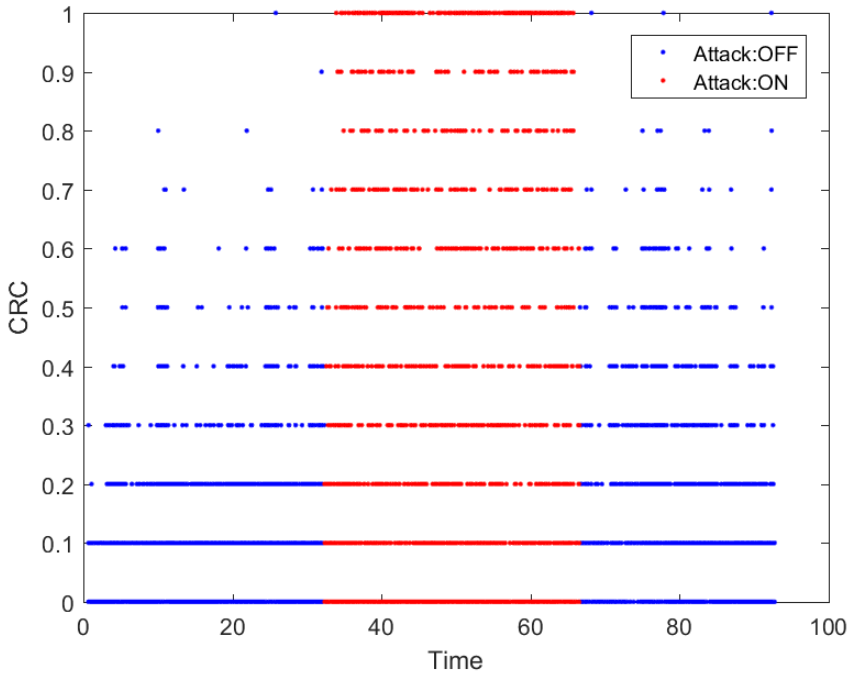


Fig. 4.28 Metric for IEEE802.11 Scenario 2 - CRC

The CRC metric remains the worst option with a higher Type-I error cases represented by the FPR value of ∼15.03%. Excluding the individual metrics, the number of metric combinations with poor performance equal to 0% DR has increased to 15, due to the addition of a secondary client host into this scenario.

The detection algorithm now is fed with data frames coming from two different nodes, increasing complexity for producing the normality pattern and leading to higher values of

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	7.931%	92.069%	68.845%	81.548%	NAV
98.549%	1.451%	63.589%	36.157%	21.360%	35.110%	$\Delta Time$
98.549%	1.451%	63.589%	36.157%	21.360%	35.110%	$\Delta Time, NAV$
14.839%	85.161%	17.036%	68.038%	13.244%	13.996%	$\Delta Time, DiffFSN, NAV$
2.765%	97.235%	6.844%	76.115%	6.612%	3.899%	DiffFSN, NAV
2.719%	97.281%	16.511%	66.440%	2.805%	2.762%	$\Delta Time, DiffFSN$
2.274%	97.726%	6.571%	76.302%	5.719%	3.254%	DiffFSN
1.577%	98.423%	3.825%	78.926%	6.739%	2.556%	$\Delta Time, T, DiffFSN, NAV$
1.021%	98.979%	1.946%	80.707%	8.420%	1.821%	T, DiffFSN, NAV
0.986%	99.014%	3.655%	78.992%	4.513%	1.618%	$\Delta Time, T, DiffFSN$
0.409%	99.591%	13.675%	68.871%	0.522%	0.459%	T, NAV
0.409%	99.591%	19.880%	62.665%	0.360%	0.383%	$\Delta Time, T$
0.409%	99.591%	19.880%	62.665%	0.360%	0.383%	$\Delta Time, T, NAV$
0.030%	99.970%	1.850%	80.629%	0.286%	0.055%	T,DiffFSN
0.030%	99.970%	11.605%	70.875%	0.046%	0.036%	T
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	$\Delta Time, CRC$
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	T, CRC
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	$\Delta Time, T, CRC$
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	DiffFSN, CRC
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	$\Delta Time, DiffFSN, CRC$
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	T, DiffFSN, CRC
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	NAV, CRC
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	$\Delta Time, NAV, CRC$
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	T, NAV, CRC
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	$\Delta Time, T, NAV, CRC$
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	DiffFSN, NAV, CRC
0.000%	100.000%	0.000%	82.474%	0.000%	0.000%	$\Delta Time, DiffFSN, NAV, CRC$
0.000%	100.000%	0.050%	82.423%	0.000%	0.000%	T, DiffFSN, NAV, CRC
0.000%	100.000%	0.348%	82.126%	0.000%	0.000%	$\Delta Time, T, DiffFSN, CRC$
0.000%	100.000%	0.354%	82.120%	0.000%	0.000%	$\Delta Time, T, DiffFSN, NAV, CRC$
0.000%	100.000%	15.025%	67.449%	0.000%	0.000%	CRC

Table 4.5 Results for IEEE 802.11 Scenario 2 with SW=20

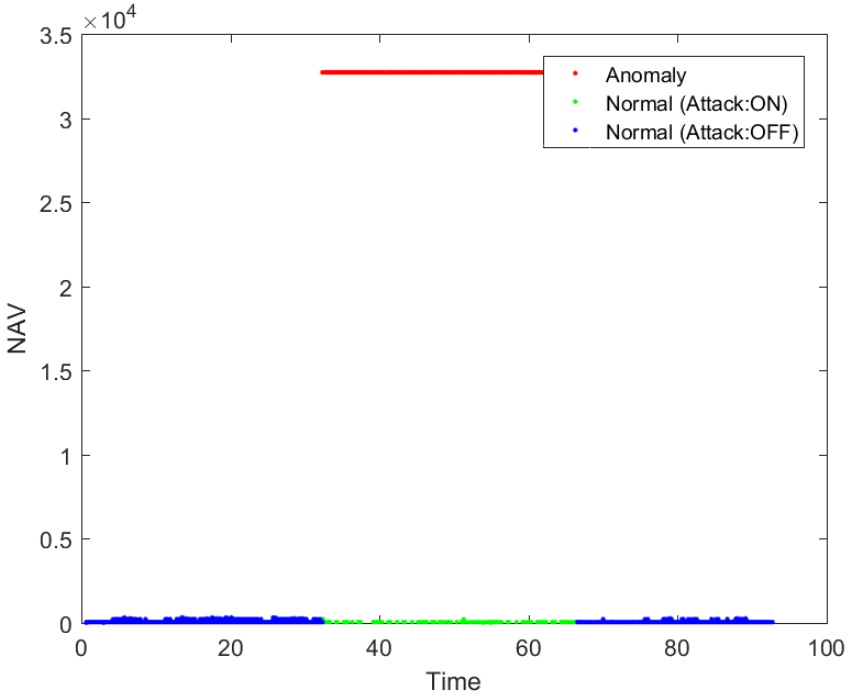


Fig. 4.29 Metric for IEEE802.11 Scenario 2 - NAV

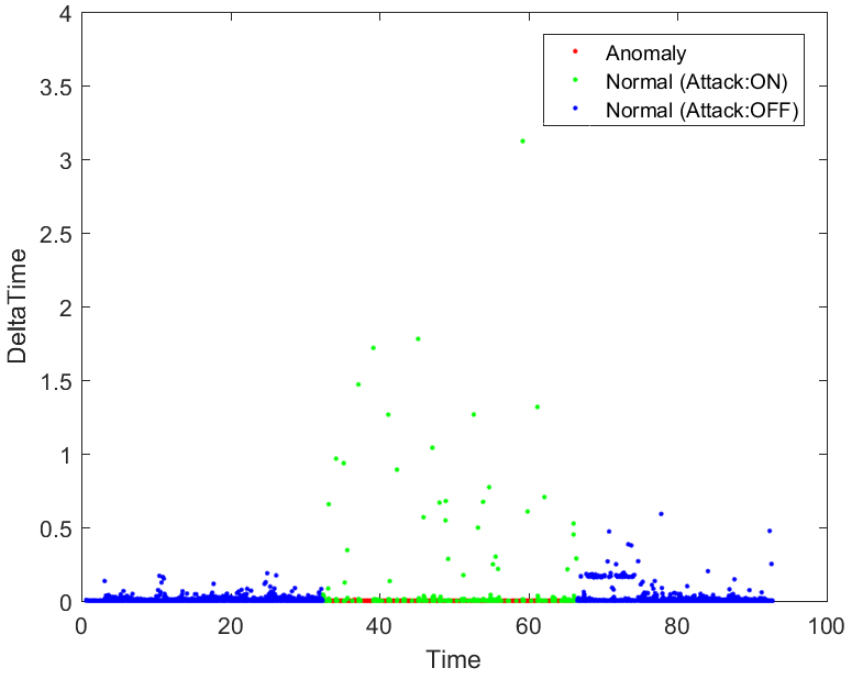


Fig. 4.30 Metric for IEEE802.11 Scenario 2 - Δ TIME

FN events. The plots for the most characteristic metrics of this scenario are displayed in the following figure 4.29, figure 4.30 and figure 4.28, with very similar patterns to the represented for Scenario 1.

Scenario 3

The results collected on this scenario represent an important improvement on the overall detection performance. Three metric combinations are able to produce a 100% DR when used individually on the detection algorithm. The highest performance remains in the NAV metric individually, with a ∼99.90% OSR value, F_1-Score of ∼99.78% and minimal detection errors with 0% FNR and only 0.1% FPR.

As it was initially predicted during the definition of the scenario, adding mobility to the node could potentially increase the number of CRC errors registered. This is the reason why on this scenario the CRC metric becomes more relevant and is able to provide a 100% DR when analysed individually, besides of misclassifying some frames as FP. The FPR value of ∼68.85% is responsible for the significant decrease of the OSR, Precision and F_1-Score indicators when comparing this metric against the NAV metric. Combining the NAV and CRC metrics does not improve the registered performance for the CRC metric individually.

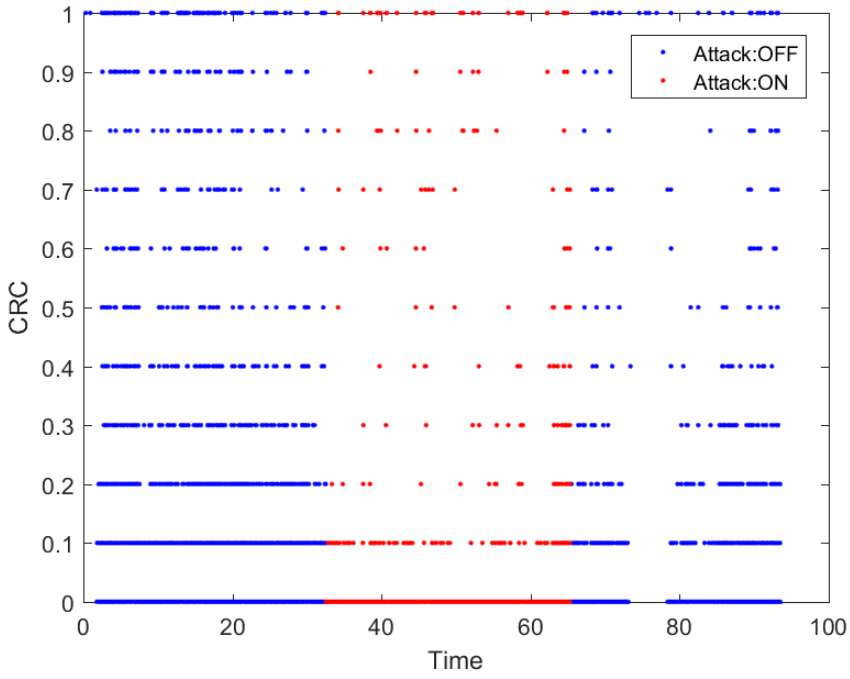


Fig. 4.31 Metric for IEEE802.11 Scenario 3 - CRC

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	0.102%	99.898%	99.555%	99.777%	NAV
100.000%	0.000%	68.852%	31.148%	24.968%	39.959%	CRC
100.000%	0.000%	68.852%	31.148%	24.968%	39.959%	NAV, CRC
82.749%	17.251%	55.802%	40.246%	25.359%	38.822%	$\Delta Time$
82.749%	17.251%	55.802%	40.246%	25.359%	38.822%	$\Delta Time, NAV$
82.749%	17.251%	55.802%	40.246%	25.359%	38.822%	$\Delta Time, CRC$
82.749%	17.251%	55.802%	40.246%	25.359%	38.822%	$\Delta Time, NAV, CRC$
53.036%	46.964%	1.863%	87.377%	86.708%	65.815%	$\Delta Time, T, NAV$
53.036%	46.964%	1.863%	87.377%	86.708%	65.815%	T, NAV, CRC
53.036%	46.964%	26.446%	62.793%	31.482%	39.510%	$\Delta Time, T, CRC$
53.036%	46.964%	26.446%	62.793%	31.482%	39.510%	$\Delta Time, T, NAV, CRC$
3.609%	96.391%	1.854%	76.062%	30.839%	6.462%	T
3.609%	96.391%	1.854%	76.062%	30.839%	6.462%	$\Delta Time, T$
3.609%	96.391%	1.854%	76.062%	30.839%	6.462%	T, NAV
3.609%	96.391%	1.854%	76.062%	30.839%	6.462%	T, CRC
0.629%	99.371%	26.702%	50.531%	0.537%	0.580%	DiffFSN
0.629%	99.371%	26.702%	50.531%	0.537%	0.580%	DiffFSN, NAV
0.629%	99.371%	26.702%	50.531%	0.537%	0.580%	DiffFSN, CRC
0.629%	99.371%	26.702%	50.531%	0.537%	0.580%	DiffFSN, NAV, CRC
0.547%	99.453%	12.807%	64.407%	0.970%	0.700%	$\Delta Time, T, DiffFSN, NAV, CRC$
0.538%	99.462%	22.550%	54.662%	0.544%	0.541%	$\Delta Time, DiffFSN$
0.538%	99.462%	22.550%	54.662%	0.544%	0.541%	$\Delta Time, DiffFSN, NAV$
0.538%	99.462%	22.550%	54.662%	0.544%	0.541%	$\Delta Time, DiffFSN, CRC$
0.538%	99.462%	22.550%	54.662%	0.544%	0.541%	$\Delta Time, DiffFSN, NAV, CRC$
0.401%	99.599%	1.187%	75.993%	7.190%	0.760%	T, DiffFSN, NAV
0.401%	99.599%	12.805%	64.375%	0.713%	0.514%	$\Delta Time, T, DiffFSN$
0.401%	99.599%	12.805%	64.375%	0.713%	0.514%	$\Delta Time, T, DiffFSN, NAV$
0.401%	99.599%	12.805%	64.375%	0.713%	0.514%	T, DiffFSN, CRC
0.401%	99.599%	12.805%	64.375%	0.713%	0.514%	$\Delta Time, T, DiffFSN, CRC$
0.401%	99.599%	12.805%	64.375%	0.713%	0.514%	T, DiffFSN, NAV, CRC
0.036%	99.964%	1.179%	75.919%	0.704%	0.069%	T,DiffFSN

Table 4.6 Results for IEEE 802.11 Scenario 3 with SW=20

On the forth position, the Δ Time metric obtains a ∼82.75% DR with a higher OSR of ∼40.25%, improving the precision offered by the CRC or (NAV, CRC) metric combinations. Furthermore, the F_1-Score only decreases by 1%, a clear indicator of how effective this metric is on this scenario.

Looking at the representation of the values registered on the CRC metric, it is possible to identify a notorious increment on the CRC errors registered, with higher CRC values recorded on figure 4.31.

Scenario 4

The predomination of the NAV metric is clear with a 100% DR and only 2.98% FPR, leading to a very high OSR , with a value of 97.02%. The second best DR value is equally registered for the Δ Time metric when analysed individually or in combination with the NAV metric.

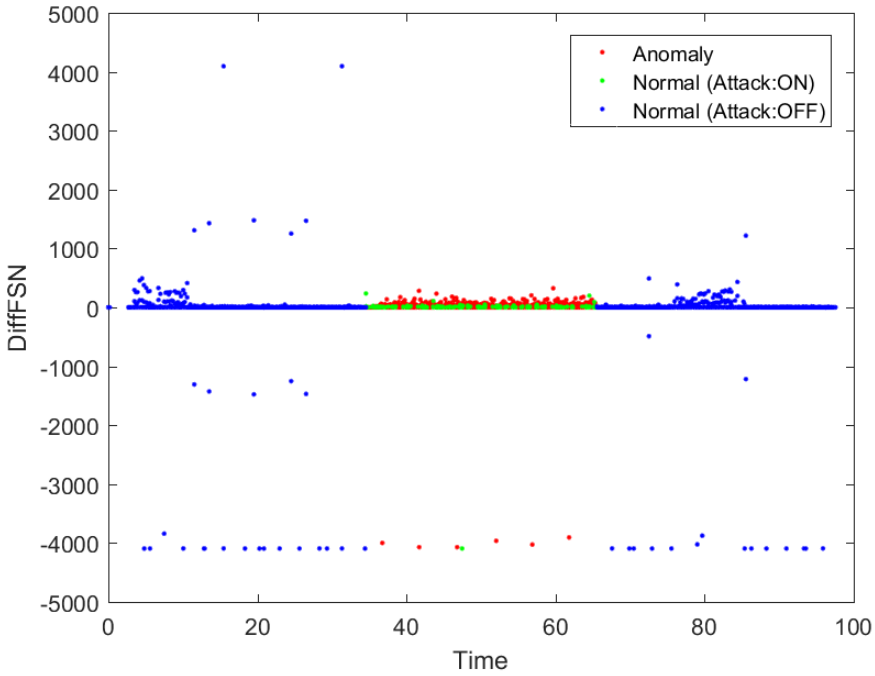


Fig. 4.32 Metric for IEEE802.11 Scenario 4 - DiffFSN

The main change on this scenario is the modest ∼29.66% DR registered by the DiffFSN metric, no matter if used individually or in combination with the NAV metric. This scenario includes two different mobile nodes, increasing the chances of delays in the transmissions, and potential frame lost or corruption when both nodes attempt to occupy the channel at the same time. This phenomenon is also represented in the lower DR registered when using the CRC

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	2.980%	97.020%	62.869%	77.202%	NAV
79.151%	20.849%	68.884%	30.064%	5.481%	10.251%	$\Delta Time$
79.151%	20.849%	68.884%	30.064%	5.481%	10.251%	$\Delta Time, NAV$
29.659%	70.341%	19.591%	76.859%	7.097%	11.454%	DiffFSN
29.659%	70.341%	19.591%	76.859%	7.097%	11.454%	DiffFSN, NAV
23.351%	76.649%	18.003%	78.129%	6.143%	9.727%	$\Delta Time, DiffFSN$
23.351%	76.649%	18.003%	78.129%	6.143%	9.727%	$\Delta Time, DiffFSN, NAV$
3.882%	96.118%	2.974%	92.175%	6.179%	4.768%	$\Delta Time, T, NAV$
3.169%	96.831%	6.517%	88.597%	2.395%	2.728%	$\Delta Time, T, DiffFSN, NAV$
1.213%	98.787%	5.430%	89.585%	1.115%	1.162%	T, DiffFSN, NAV
1.213%	98.787%	6.517%	88.498%	0.931%	1.053%	$\Delta Time, T, DiffFSN$
0.334%	99.666%	5.151%	89.820%	0.326%	0.330%	T,DiffFSN
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	$\Delta Time, CRC$
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	T, CRC
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	$\Delta Time, T, CRC$
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	DiffFSN, CRC
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	$\Delta Time, DiffFSN, CRC$
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	T, DiffFSN, CRC
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	NAV, CRC
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	$\Delta Time, NAV, CRC$
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	T, NAV, CRC
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	$\Delta Time, T, NAV, CRC$
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	DiffFSN, NAV, CRC
0.000%	100.000%	0.000%	94.954%	0.000%	0.000%	$\Delta Time, DiffFSN, NAV, CRC$
0.000%	100.000%	0.018%	94.936%	0.000%	0.000%	T, DiffFSN, NAV, CRC
0.000%	100.000%	0.065%	94.889%	0.000%	0.000%	$\Delta Time, T, DiffFSN, CRC$
0.000%	100.000%	0.068%	94.886%	0.000%	0.000%	$\Delta Time, T, DiffFSN, NAV, CRC$
0.000%	100.000%	0.121%	94.833%	0.000%	0.000%	T
0.000%	100.000%	0.152%	94.802%	0.000%	0.000%	T, NAV
0.000%	100.000%	0.213%	94.741%	0.000%	0.000%	$\Delta Time, T$
0.000%	100.000%	17.494%	77.459%	0.000%	0.000%	CRC

Table 4.7 Results for IEEE 802.11 Scenario 4 with SW=20

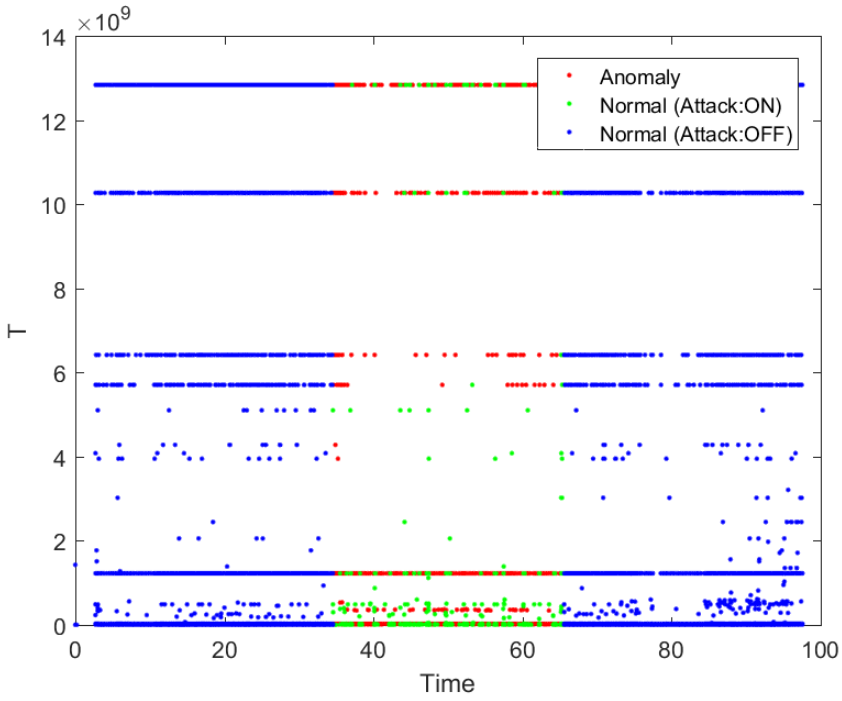


Fig. 4.33 Metric for IEEE802.11 Scenario 4 - T

metric or the combination of (Δ Time, T), as the throughput fluctuates more with the constant movement of both client nodes leading to an increase in the detection errors.

Figure 4.32 and figure 4.33 represent the values registered for the DiffFSN and T metric, respectively.

Scenario 5

In a similar manner to Scenario 3, the outperforming metrics are the NAV and CRC, no matter if they are analysed individually or combined. The Δ Time metric provides a ∼80.83% DR, registering the same performance when combined with the NAV and/or CRC metrics. However, only the NAV metric is able to provide accuracy with ∼97.38% OSR and ∼82.63% precision on the detection, while all the other aforementioned metric combinations only provide OSR values below 25% with a Precision smaller than 15%.

The main reason to explain the lack of strong detection accuracy, whenever the DR falls within acceptable values for a unsupervised on-line IDS, is the hidden node problem. This scenario has a fixed node placed within a long distance from the AP, increasing the probabilities of suffering from this problem as a secondary mobile node comped for the same resources with an advantage position whenever it moves closer to the AP. The direct effect of the hidden node problem is an increase on the collision throughout the duration of the monitoring period, which

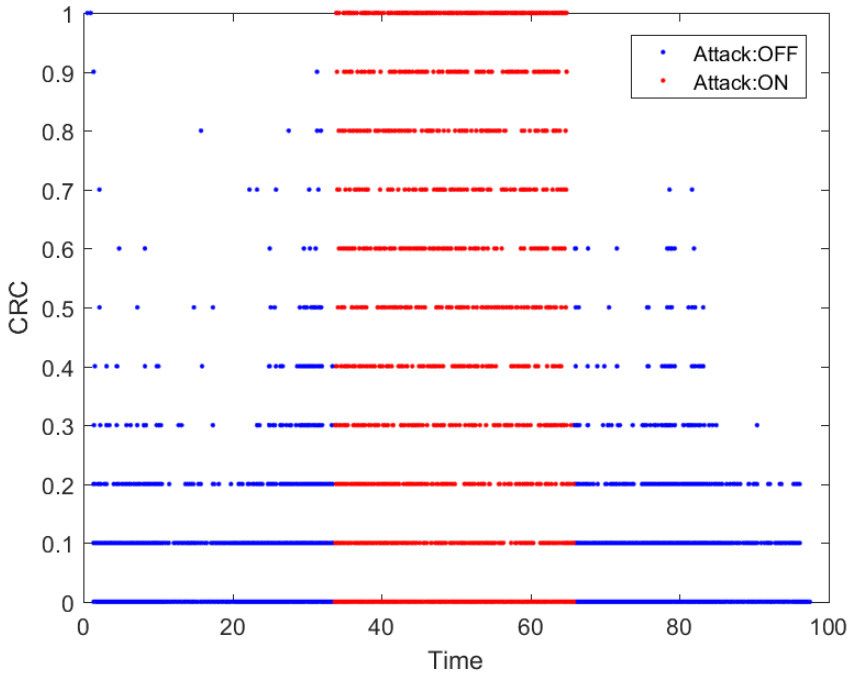


Fig. 4.34 Metric for IEEE802.11 Scenario 5 - CRC

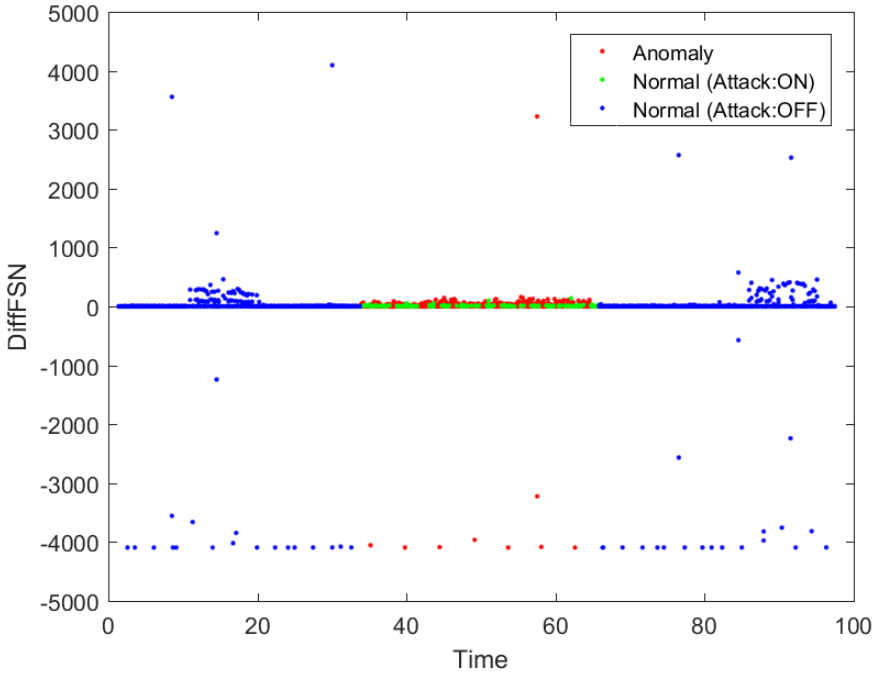


Fig. 4.35 Metric for IEEE802.11 Scenario 5 - DiffFSN

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	2.623%	97.377%	82.626%	90.487%	NAV
100.000%	0.000%	76.262%	23.738%	14.057%	24.649%	CRC
100.000%	0.000%	76.262%	23.738%	14.057%	24.649%	NAV, CRC
80.828%	19.172%	68.919%	28.690%	12.762%	22.044%	$\Delta Time$
80.828%	19.172%	68.919%	28.690%	12.762%	22.044%	$\Delta Time, NAV$
80.828%	19.172%	68.919%	28.690%	12.762%	22.044%	$\Delta Time, CRC$
80.828%	19.172%	68.919%	28.690%	12.762%	22.044%	$\Delta Time, NAV, CRC$
29.019%	70.981%	29.224%	61.922%	11.021%	15.975%	$\Delta Time, T, NAV$
29.019%	70.981%	29.224%	61.922%	11.021%	15.975%	T, NAV, CRC
29.019%	70.981%	38.560%	52.586%	8.582%	13.246%	$\Delta Time, T, CRC$
29.019%	70.981%	38.560%	52.586%	8.582%	13.246%	$\Delta Time, T, NAV, CRC$
16.663%	83.337%	20.183%	69.422%	9.337%	11.968%	DiffFSN
16.663%	83.337%	20.183%	69.422%	9.337%	11.968%	DiffFSN, NAV
16.663%	83.337%	20.183%	69.422%	9.337%	11.968%	DiffFSN, CRC
16.663%	83.337%	20.183%	69.422%	9.337%	11.968%	DiffFSN, NAV, CRC
13.614%	86.386%	18.776%	70.449%	8.294%	10.308%	$\Delta Time, DiffFSN$
13.614%	86.386%	18.776%	70.449%	8.294%	10.308%	$\Delta Time, DiffFSN, NAV$
13.614%	86.386%	18.776%	70.449%	8.294%	10.308%	$\Delta Time, DiffFSN, CRC$
13.614%	86.386%	18.776%	70.449%	8.294%	10.308%	$\Delta Time, DiffFSN, NAV, CRC$
11.817%	88.183%	16.784%	72.216%	8.073%	9.593%	$\Delta Time, T, DiffFSN, NAV, CRC$
6.241%	93.759%	12.648%	75.658%	5.799%	6.012%	$\Delta Time, T, DiffFSN, NAV$
6.241%	93.759%	12.648%	75.658%	5.799%	6.012%	T, DiffFSN, NAV, CRC
6.241%	93.759%	15.100%	73.204%	4.903%	5.492%	$\Delta Time, T, DiffFSN, CRC$
4.823%	95.177%	6.998%	81.131%	7.917%	5.994%	T, DiffFSN, NAV
4.823%	95.177%	12.648%	75.481%	4.541%	4.678%	$\Delta Time, T, DiffFSN$
4.823%	95.177%	12.648%	75.481%	4.541%	4.678%	T, DiffFSN, CRC
3.445%	96.555%	29.210%	58.746%	1.450%	2.041%	T
3.445%	96.555%	29.210%	58.746%	1.450%	2.041%	$\Delta Time, T$
3.445%	96.555%	29.210%	58.746%	1.450%	2.041%	T, NAV
3.445%	96.555%	29.210%	58.746%	1.450%	2.041%	T, CRC
1.476%	98.524%	6.985%	80.725%	2.568%	1.874%	T,DiffFSN

Table 4.8 Results for IEEE 802.11 Scenario 5 with SW=20

can be observed on figure 4.34 where the CRC metric is represented. This problem also have a lower impact on the DiffFSN metric, as shown in figure 4.35.

Scenario 6

The similarities between Scenario 6 and the previous results obtained on Scenario 5 is obvious, and can be easily understood by looking at the changes applied on the definition of each scenario. In Scenario 6, the mobile node remains intact, whereas the fixed node is moved to a position 5 times closer to the AP. The hidden node problem reduces its probability considerably, and it has a direct effect on the results obtained for the NAV metric, with a minimal 2.18% FPR with 100% DR.

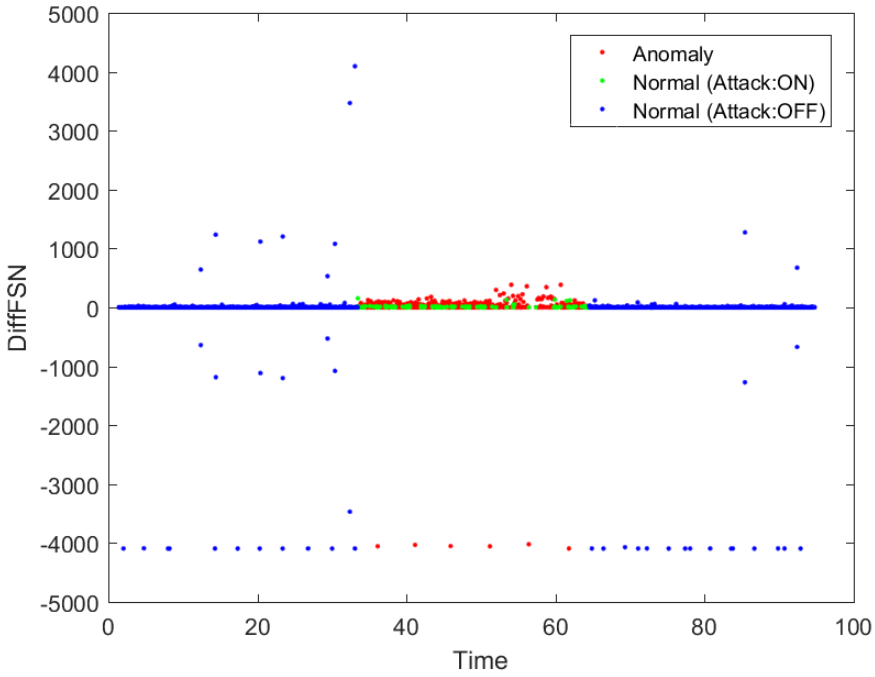


Fig. 4.36 Metric for IEEE802.11 Scenario 6 - DiffFSN

The CRC metric is able to register 100% DR when evaluated independently or in combination with the NAV metric, although the FPR increases by 3% in comparison with the previous scenario. On the contrary, the combinations including the Δ Time metric suffer a general improvement on its performance and accuracy, with a lower FNR rate which causes an increase of nearly 8% for the best case, the metric set of (Δ Time, NAV).

The worse performance is obtained when using the T metric, with a small ∼2.78% DR and very high FNR/FPR, with a value of 97.22% and 36.48% respectively. A slightly improvement can be seen in the representation of the DiffFSN metric on figure 4.36.The T metric, plotted

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	2.180%	97.820%	63.625%	77.769%	NAV
100.000%	0.000%	79.704%	20.296%	4.565%	8.731%	CRC
100.000%	0.000%	79.704%	20.296%	4.565%	8.731%	NAV, CRC
98.398%	1.602%	63.578%	36.361%	5.571%	10.546%	$\Delta Time, NAV$
98.398%	1.602%	71.825%	28.113%	4.963%	9.450%	$\Delta Time, CRC$
98.398%	1.602%	71.825%	28.113%	4.963%	9.450%	$\Delta Time, NAV, CRC$
75.671%	24.329%	63.542%	35.530%	4.343%	8.214%	$\Delta Time$
56.986%	43.014%	45.340%	53.020%	4.572%	8.465%	$\Delta Time, T, NAV$
56.986%	43.014%	52.978%	45.382%	3.939%	7.369%	T, NAV, CRC
56.986%	43.014%	64.295%	34.065%	3.268%	6.182%	$\Delta Time, T, CRC$
56.986%	43.014%	64.295%	34.065%	3.268%	6.182%	$\Delta Time, T, NAV, CRC$
48.342%	51.658%	36.567%	61.464%	4.798%	8.730%	T, NAV
48.342%	51.658%	52.928%	45.103%	3.365%	6.292%	T, CRC
46.740%	53.260%	45.049%	52.920%	3.805%	7.037%	$\Delta Time, T$
36.494%	63.506%	16.973%	80.606%	7.576%	12.547%	DiffFSN
36.494%	63.506%	16.973%	80.606%	7.576%	12.547%	DiffFSN, NAV
36.494%	63.506%	16.973%	80.606%	7.576%	12.547%	DiffFSN, CRC
36.494%	63.506%	16.973%	80.606%	7.576%	12.547%	DiffFSN, NAV, CRC
35.898%	64.102%	15.564%	81.993%	8.082%	13.194%	$\Delta Time, DiffFSN$
35.898%	64.102%	15.564%	81.993%	8.082%	13.194%	$\Delta Time, DiffFSN, NAV$
35.898%	64.102%	15.564%	81.993%	8.082%	13.194%	$\Delta Time, DiffFSN, CRC$
35.898%	64.102%	15.564%	81.993%	8.082%	13.194%	$\Delta Time, DiffFSN, NAV, CRC$
30.496%	69.504%	12.682%	84.668%	8.397%	13.168%	$\Delta Time, T, DiffFSN, NAV, CRC$
29.937%	70.063%	11.184%	86.145%	9.260%	14.144%	T, DiffFSN, NAV, CRC
21.498%	78.502%	9.316%	87.691%	8.086%	11.752%	T, DiffFSN, NAV
21.498%	78.502%	11.180%	85.827%	6.830%	10.366%	$\Delta Time, T, DiffFSN$
21.498%	78.502%	11.180%	85.827%	6.830%	10.366%	$\Delta Time, T, DiffFSN, NAV$
21.498%	78.502%	11.180%	85.827%	6.830%	10.366%	T, DiffFSN, CRC
21.498%	78.502%	11.190%	85.818%	6.824%	10.360%	$\Delta Time, T, DiffFSN, CRC$
19.449%	80.551%	9.311%	87.618%	7.375%	10.695%	T,DiffFSN
2.776%	97.224%	36.487%	59.807%	0.289%	0.524%	T

Table 4.9 Results for IEEE 802.11 Scenario 6 with SW=20

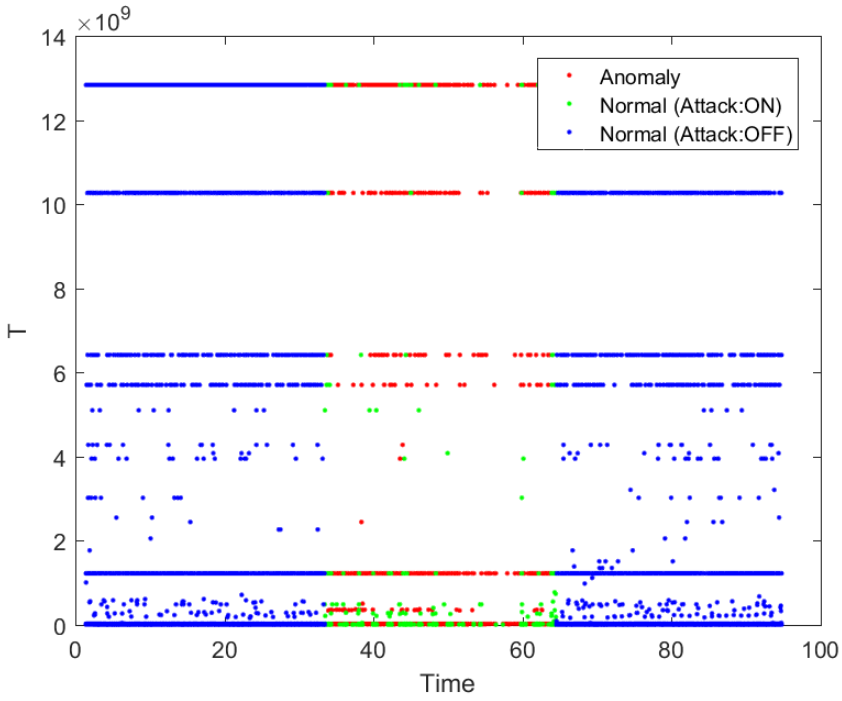


Fig. 4.37 Metric for IEEE802.11 Scenario 6 - T

on figure 4.37 does not provide a clear distinction between the values registered during the attacking phase and the initial/normal phases, explaining why the individual use of this metric does not provide successful detection results.

Scenario 7

The major novelty on this case is the incorporation of the RTS/CTS mechanism in the single active node of this scenario. This mechanism has a clear impact on the most efficient metric identified for this case: NAV, Δ Time and T. The three metrics have been represented in figure 4.38, figure 4.39 and figure 4.40.

The combinations of the Δ Time metric with the NAV metric does not have any impact on its performance. Similarly, the four combinations evaluated with the T metric: (Δ Time, T), (T, NAV) and (Δ Time, T, NAV); matches their detection performance and accuracy, with a ∼67.05% DR and ∼55.47% OSR. The FNR and FPR values remain within the 30-40% interval.

Since the RTS/CTS mechanism aims at preventing collisions from happening, it is expected for the CRC metric to play a secondary role on this scenario. The highest DR is reached with the metric combination (Δ Time, T, DiffFSN, NAV).

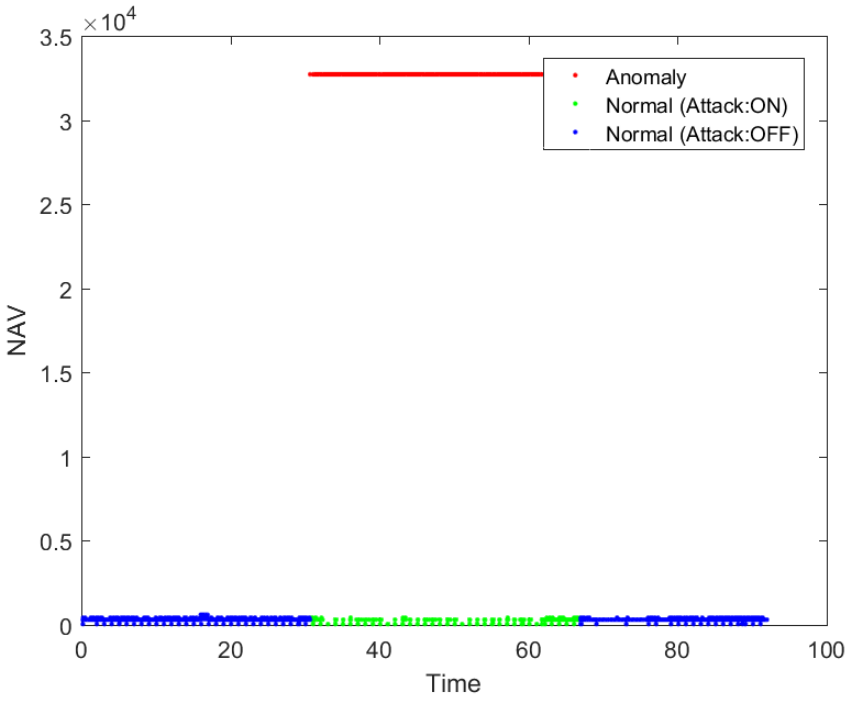


Fig. 4.38 Metric for IEEE802.11 Scenario 7 - NAV

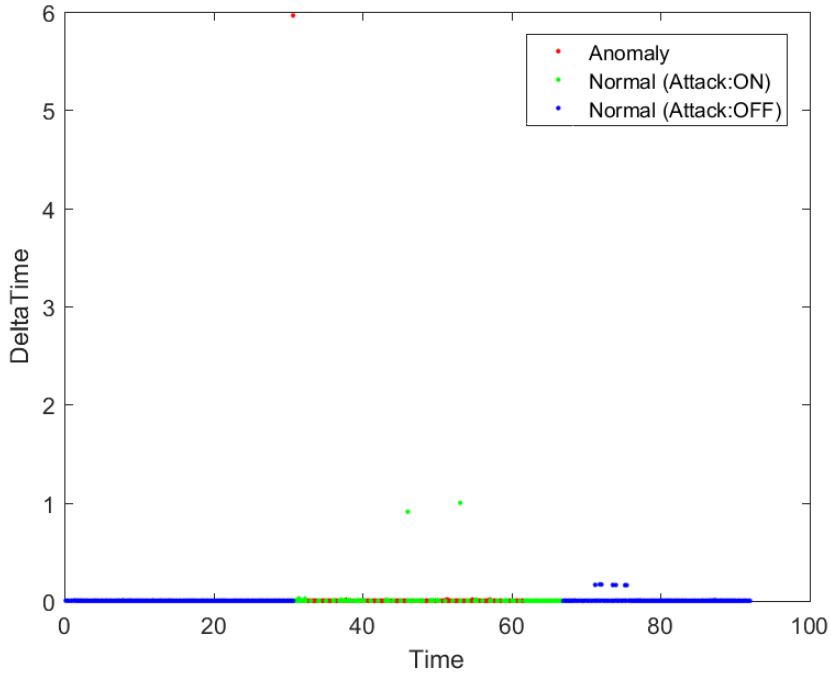


Fig. 4.39 Metric for IEEE802.11 Scenario 7 - Δ TIME

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	1.733%	98.267%	93.892%	96.850%	NAV
85.880%	14.120%	60.023%	36.215%	27.597%	41.771%	$\Delta Time$
85.880%	14.120%	60.023%	36.215%	27.597%	41.771%	$\Delta Time, NAV$
67.052%	32.948%	35.751%	55.472%	33.317%	44.515%	T
67.052%	32.948%	35.751%	55.472%	33.317%	44.515%	$\Delta Time, T$
67.052%	32.948%	35.751%	55.472%	33.317%	44.515%	T, NAV
67.052%	32.948%	35.751%	55.472%	33.317%	44.515%	$\Delta Time, T, NAV$
1.905%	98.095%	9.988%	63.880%	4.836%	2.734%	DiffFSN
1.905%	98.095%	9.988%	63.880%	4.836%	2.734%	DiffFSN, NAV
1.595%	98.405%	7.897%	65.889%	5.107%	2.431%	$\Delta Time, DiffFSN$
1.595%	98.405%	7.897%	65.889%	5.107%	2.431%	$\Delta Time, DiffFSN, NAV$
1.272%	98.728%	4.754%	68.945%	6.655%	2.136%	$\Delta Time, T, DiffFSN, NAV$
1.266%	98.734%	4.075%	69.623%	7.642%	2.172%	T, DiffFSN, NAV
1.266%	98.734%	4.745%	68.952%	6.635%	2.126%	$\Delta Time, T, DiffFSN$
1.263%	98.737%	2.995%	70.702%	10.097%	2.245%	$\Delta Time, T, DiffFSN, NAV, CRC$
1.263%	98.737%	4.062%	69.635%	7.647%	2.167%	T,DiffFSN
0.444%	99.556%	0.043%	73.436%	73.514%	0.882%	T, DiffFSN, NAV, CRC
0.444%	99.556%	2.891%	70.588%	3.928%	0.797%	$\Delta Time, T, DiffFSN, CRC$
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	$\Delta Time, CRC$
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	T, CRC
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	$\Delta Time, T, CRC$
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	DiffFSN, CRC
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	$\Delta Time, DiffFSN, CRC$
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	T, DiffFSN, CRC
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	NAV, CRC
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	$\Delta Time, NAV, CRC$
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	T, NAV, CRC
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	$\Delta Time, T, NAV, CRC$
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	DiffFSN, NAV, CRC
0.000%	100.000%	0.000%	73.361%	0.000%	0.000%	$\Delta Time, DiffFSN, NAV, CRC$
0.000%	100.000%	2.363%	70.997%	0.000%	0.000%	CRC

Table 4.10 Results for IEEE 802.11 Scenario 7 with SW=20

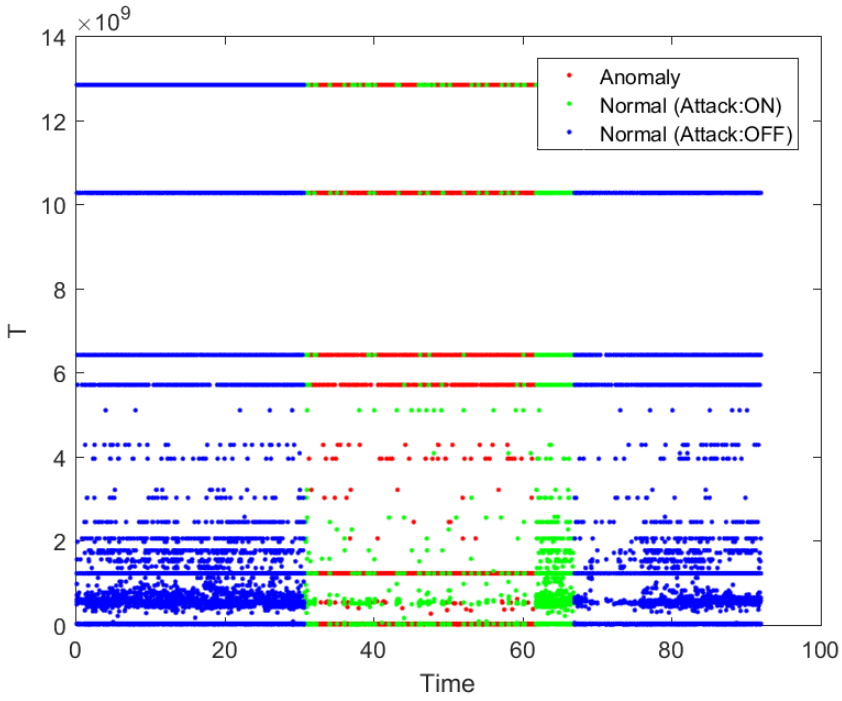


Fig. 4.40 Metric for IEEE802.11 Scenario 7 - T

Scenario 8

As previously, the most effective metrics for detecting the attack are NAV and CRC, and the combination of them into a single set of metrics. The DR is 100%, with no FN cases registered. However, when using the CRC individually or in combination with the NAV metric, the accuracy decreases due to the number of cases misclassified as FP.

This scenario is also vulnerable to the hidden node problem, as the RTS/CTS mechanism has only been enabled in the closest node to the AP located on a fixed position.

The combination of the NAV metric with the (Δ Time reduces the DR by (∼16.30%, as well as decrementing the FPR, which is compensated by an increment of the FNR that decrease the Precision of the detection.

The high values of FNR and FPR are self-explained when observing the figure 4.41 and figure 4.42, were minimal differences can be identified for the attacker traffic and the normal traffic (prior and during the attacking phase), in a quick look at the metric values registered.

Figure 4.43 shows the level of uncertainty inflicted by the T metric, with the worse performance obtained for this scenario when combined with the DiffFSN metric. The DR and accuracy only offer a slightly better performance whenever the DiffFSN metric is used individually.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	21.582%	78.418%	45.948%	62.965%	NAV
100.000%	0.000%	69.363%	30.637%	20.917%	34.597%	CRC
100.000%	0.000%	69.363%	30.637%	20.917%	34.597%	NAV, CRC
83.706%	16.294%	53.807%	43.204%	22.203%	35.097%	$\Delta Time, NAV$
83.706%	16.294%	60.269%	36.742%	20.306%	32.684%	$\Delta Time, CRC$
83.706%	16.294%	60.269%	36.742%	20.306%	32.684%	$\Delta Time, NAV, CRC$
65.996%	34.004%	50.565%	43.197%	19.319%	29.888%	$\Delta Time$
50.397%	49.603%	38.815%	52.085%	19.238%	27.846%	T, NAV, CRC
37.188%	62.812%	28.345%	60.132%	19.400%	25.498%	T, NAV
37.188%	62.812%	34.471%	54.005%	16.522%	22.879%	T, CRC
34.103%	65.897%	29.720%	58.191%	17.391%	23.035%	$\Delta Time, T, NAV$
34.103%	65.897%	39.264%	48.647%	13.744%	19.592%	$\Delta Time, T, CRC$
34.103%	65.897%	39.265%	48.646%	13.744%	19.592%	$\Delta Time, T, NAV, CRC$
20.894%	79.106%	25.370%	60.118%	13.126%	16.123%	T
20.894%	79.106%	25.377%	60.111%	13.123%	16.121%	$\Delta Time, T$
4.715%	95.285%	10.764%	71.754%	7.437%	5.771%	$\Delta Time, T, DiffFSN, NAV, CRC$
2.336%	97.664%	15.872%	66.210%	2.629%	2.474%	DiffFSN, NAV, CRC
1.987%	98.013%	15.354%	66.665%	2.319%	2.140%	$\Delta Time, DiffFSN, NAV, CRC$
1.634%	98.366%	13.510%	68.444%	2.170%	1.864%	$\Delta Time, DiffFSN, NAV$
1.634%	98.366%	15.303%	66.651%	1.921%	1.766%	$\Delta Time, DiffFSN, CRC$
1.041%	98.959%	8.517%	73.329%	2.193%	1.412%	T, DiffFSN, NAV, CRC
0.733%	99.267%	6.938%	74.852%	1.902%	1.058%	T, DiffFSN, NAV
0.733%	99.267%	8.108%	73.682%	1.632%	1.012%	T, DiffFSN, CRC
0.688%	99.312%	7.257%	74.524%	1.709%	0.981%	$\Delta Time, T, DiffFSN, NAV$
0.688%	99.312%	9.127%	72.653%	1.363%	0.914%	$\Delta Time, T, DiffFSN, CRC$
0.653%	99.347%	6.823%	74.952%	1.727%	0.948%	$\Delta Time, T, DiffFSN$
0.456%	99.544%	7.416%	74.322%	1.115%	0.647%	DiffFSN, NAV
0.456%	99.544%	15.473%	66.265%	0.538%	0.493%	DiffFSN, CRC
0.395%	99.605%	12.952%	68.774%	0.557%	0.462%	$\Delta Time, DiffFSN$
0.338%	99.662%	5.714%	76.002%	1.074%	0.514%	DiffFSN
0.304%	99.696%	6.594%	75.116%	0.838%	0.446%	T,DiffFSN

Table 4.11 Results for IEEE 802.11 Scenario 8 with SW=20

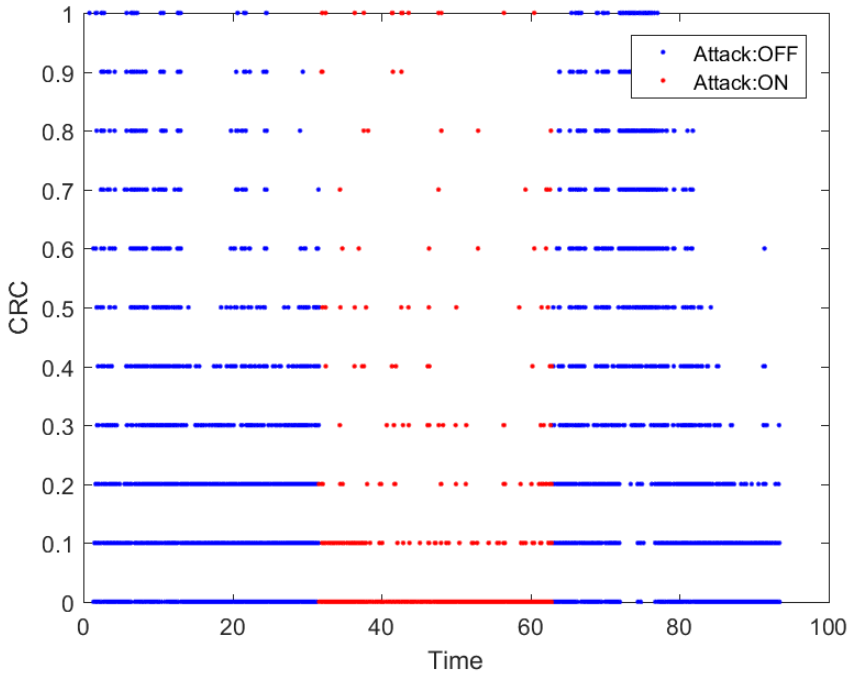


Fig. 4.41 Metric for IEEE802.11 Scenario 8 - CRC

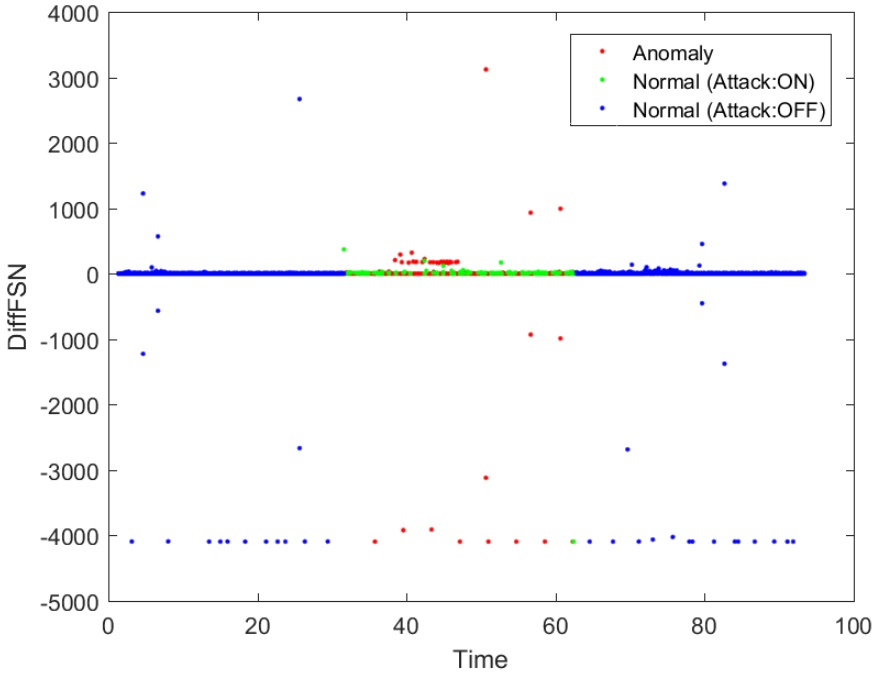


Fig. 4.42 Metric for IEEE802.11 Scenario 8 - DiffFSN

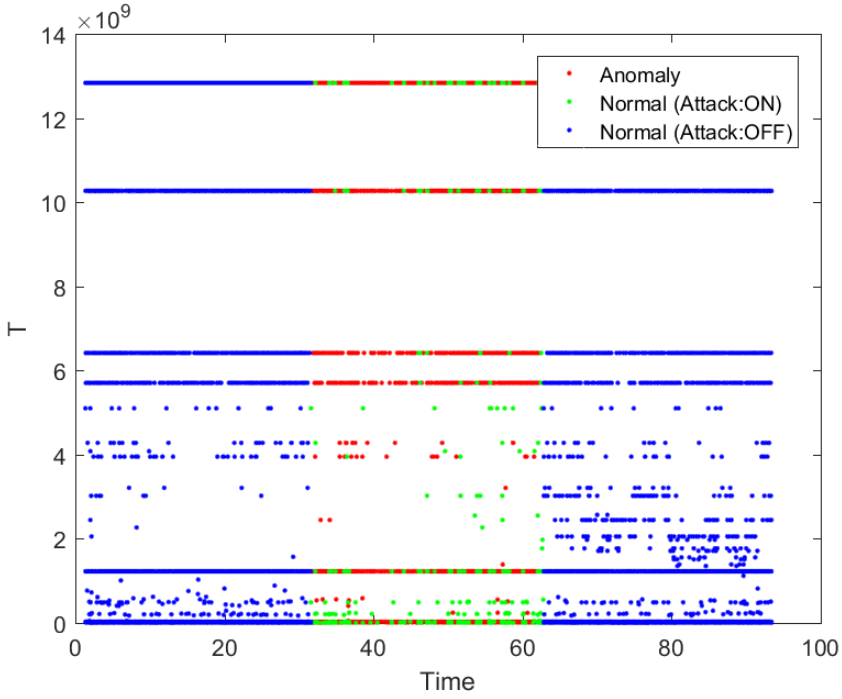


Fig. 4.43 Metric for IEEE802.11 Scenario 8 - T

Scenario 9

During the definition of this scenario, the benefits of enabling the RTS/CTS mechanism in all the active clients were described. This effect is the reason why the detection performance suffers an important improvement in comparison with Scenario 8.

However, the highest F_1-Score value is not registered when using the NAV metric on this occasion, as it is obtained when evaluating the set of metrics composed by the combination (Δ Time, NAV, CRC). The OSR value is ∼69.03%, 4% below the value obtained when using NAV metric individually.

The minimum DR obtained occurs when using the (Δ Time, DiffFSN) metric combination. Figure 4.44 and figure 4.45 represent the values obtained for these two metrics, where the DiffFSN values are very similar for normal and attack frames through all the attacking phase.

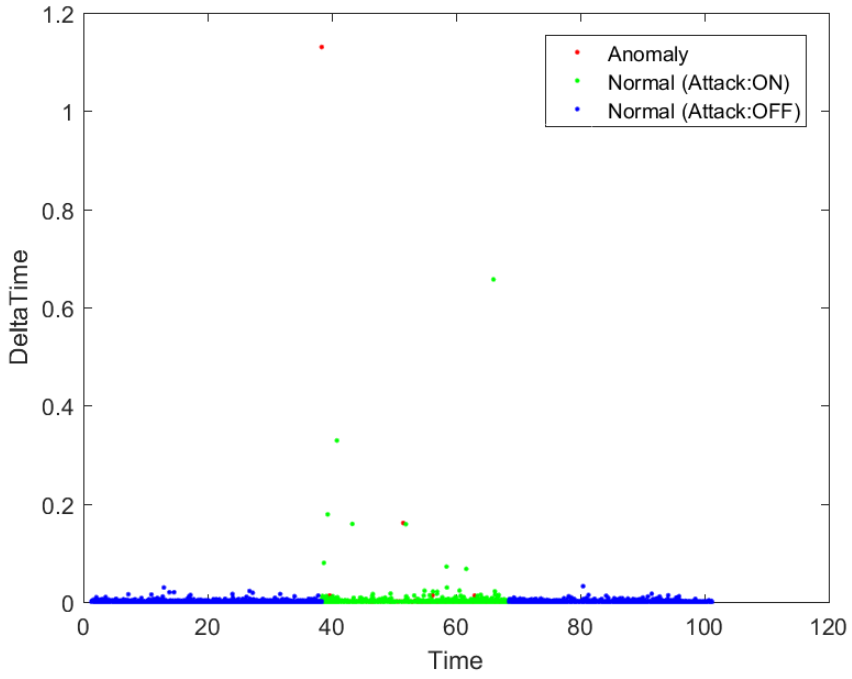


Fig. 4.44 Metric for IEEE802.11 Scenario 9 - Δ TIME

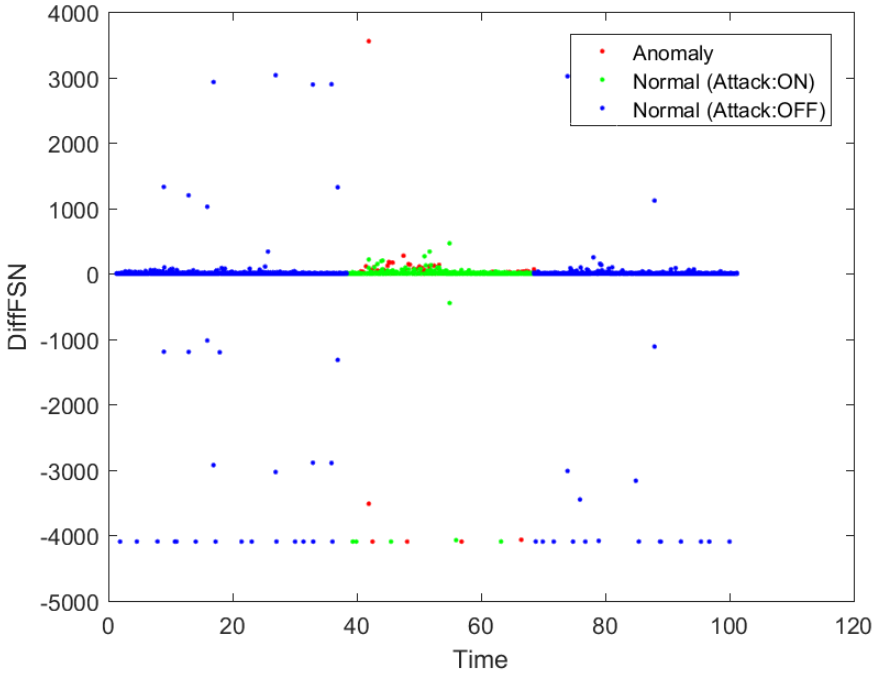


Fig. 4.45 Metric for IEEE802.11 Scenario 9 - DiffFSN

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	34.703%	65.297%	20.777%	34.406%	NAV
100.000%	0.000%	34.703%	65.297%	20.777%	34.406%	NAV, CRC
100.000%	0.000%	81.489%	18.512%	10.047%	18.259%	CRC
91.027%	8.973%	30.157%	69.026%	21.551%	34.851%	$\Delta Time, NAV$
91.027%	8.973%	30.157%	69.026%	21.551%	34.851%	$\Delta Time, NAV, CRC$
91.027%	8.973%	69.941%	29.242%	10.591%	18.974%	$\Delta Time$
91.027%	8.973%	69.941%	29.242%	10.591%	18.974%	$\Delta Time, CRC$
43.952%	56.048%	16.660%	78.239%	19.362%	26.882%	$\Delta Time, T, NAV$
43.952%	56.048%	16.660%	78.239%	19.362%	26.882%	T, NAV, CRC
43.952%	56.048%	16.660%	78.239%	19.362%	26.882%	$\Delta Time, T, NAV, CRC$
43.952%	56.048%	40.778%	54.121%	8.933%	14.849%	$\Delta Time, T, CRC$
28.079%	71.921%	11.888%	81.567%	17.694%	21.708%	T, NAV
28.079%	71.921%	33.086%	60.368%	7.170%	11.423%	$\Delta Time, T$
28.079%	71.921%	33.086%	60.368%	7.170%	11.423%	T, CRC
28.045%	71.955%	33.065%	60.386%	7.166%	11.416%	T
16.889%	83.111%	6.544%	85.891%	19.021%	17.892%	DiffFSN, NAV, CRC
15.538%	84.462%	5.852%	86.461%	19.462%	17.280%	$\Delta Time, DiffFSN, NAV$
15.538%	84.462%	5.852%	86.461%	19.462%	17.280%	$\Delta Time, DiffFSN, NAV, CRC$
15.538%	84.462%	12.852%	79.461%	9.913%	12.104%	$\Delta Time, DiffFSN, CRC$
13.355%	86.645%	5.560%	86.554%	17.941%	15.312%	$\Delta Time, T, DiffFSN, NAV, CRC$
5.129%	94.871%	3.178%	88.187%	12.807%	7.324%	T, DiffFSN, NAV
5.129%	94.871%	3.178%	88.187%	12.807%	7.324%	$\Delta Time, T, DiffFSN, NAV$
5.129%	94.871%	3.178%	88.187%	12.807%	7.324%	T, DiffFSN, NAV, CRC
5.129%	94.871%	7.976%	83.389%	5.529%	5.321%	$\Delta Time, T, DiffFSN$
5.129%	94.871%	7.976%	83.389%	5.529%	5.321%	T, DiffFSN, CRC
5.129%	94.871%	7.976%	83.389%	5.529%	5.321%	$\Delta Time, T, DiffFSN, CRC$
1.570%	98.430%	3.909%	87.132%	3.526%	2.172%	T,DiffFSN
1.284%	98.716%	1.674%	89.342%	6.527%	2.146%	DiffFSN, NAV
1.284%	98.716%	4.504%	86.511%	2.530%	1.704%	DiffFSN
1.284%	98.716%	4.504%	86.511%	2.530%	1.704%	DiffFSN, CRC
1.158%	98.842%	4.273%	86.731%	2.408%	1.564%	$\Delta Time, DiffFSN$

Table 4.12 Results for IEEE 802.11 Scenario 9 with SW=20

Scenario 10

Looking at the results presented in table 4.13, enabling the RTS/CTS mechanism in the node positioned at the farthest distance from the AP has a minimal effect on the CRC and (NAV,CRC) metric combinations. If the results obtained are compared with Scenario 8, where the RTS/CTS mechanism was enabled in the client located at a short distance from the AP, it is possible to differentiate a minor increase on the FPR accompanied by a reduction of the FNR. Obviously, these two parameters are directly related with the Type-I and Type-II errors, extending the negative effect on the parameters measuring the detection accuracy: OSR, Precision and F_1-Score.

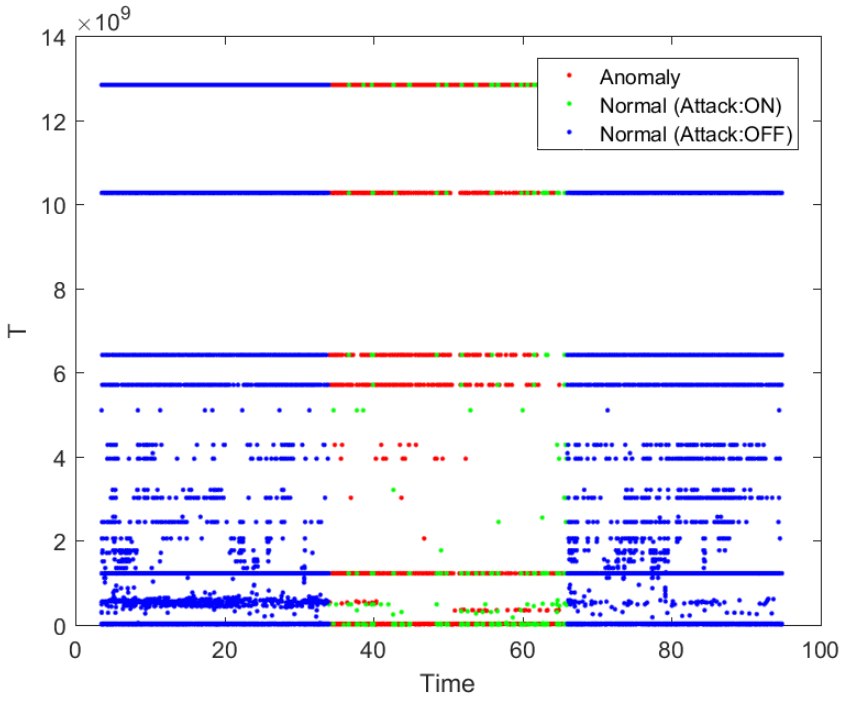


Fig. 4.46 Metric for IEEE802.11 Scenario 10 - T

On the contrary, the single NAV metric enhances its detection performance on this scenario, with a 10% reduction of the FPR value, directly translated to the OSR.

The negative effect of the T metric remains active, specially when combined with DiffFSN, CRC and/or Δ Time in metric sets of 2-3 metrics, registering a FNR close to 100% on the combination displayed towards the end of the table.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	12.894%	87.106%	50.630%	67.225%	NAV
100.000%	0.000%	80.995%	19.005%	14.034%	24.614%	CRC
100.000%	0.000%	80.995%	19.005%	14.034%	24.614%	NAV, CRC
84.209%	15.791%	64.121%	33.791%	14.796%	25.170%	$\Delta Time, NAV$
84.209%	15.791%	72.737%	25.175%	13.276%	22.936%	$\Delta Time, CRC$
84.209%	15.791%	72.737%	25.175%	13.276%	22.936%	$\Delta Time, NAV, CRC$
76.685%	23.315%	62.469%	34.448%	13.965%	23.628%	$\Delta Time$
71.698%	28.302%	42.821%	53.437%	18.127%	28.938%	T, NAV, CRC
55.907%	44.093%	41.500%	52.669%	15.120%	23.803%	$\Delta Time, T, NAV$
55.907%	44.093%	45.150%	49.020%	14.070%	22.482%	$\Delta Time, T, CRC$
55.907%	44.093%	45.150%	49.020%	14.070%	22.482%	$\Delta Time, T, NAV, CRC$
35.900%	64.100%	40.588%	50.936%	10.471%	16.213%	T, NAV
35.900%	64.100%	40.611%	50.913%	10.466%	16.207%	$\Delta Time, T$
35.900%	64.100%	40.611%	50.913%	10.466%	16.207%	T, CRC
35.873%	64.127%	40.586%	50.935%	10.465%	16.203%	T
11.030%	88.970%	7.692%	80.543%	15.939%	13.038%	$\Delta Time, T, DiffFSN, NAV, CRC$
9.693%	90.307%	9.864%	78.195%	11.500%	10.519%	DiffFSN
9.693%	90.307%	9.864%	78.195%	11.500%	10.519%	DiffFSN, NAV
9.693%	90.307%	9.864%	78.195%	11.500%	10.519%	DiffFSN, CRC
9.693%	90.307%	9.864%	78.195%	11.500%	10.519%	DiffFSN, NAV, CRC
8.315%	91.685%	9.030%	78.847%	10.855%	9.417%	$\Delta Time, DiffFSN$
8.315%	91.685%	9.030%	78.847%	10.855%	9.417%	$\Delta Time, DiffFSN, NAV$
8.315%	91.685%	9.030%	78.847%	10.855%	9.417%	$\Delta Time, DiffFSN, CRC$
8.315%	91.685%	9.030%	78.847%	10.855%	9.417%	$\Delta Time, DiffFSN, NAV, CRC$
8.036%	91.965%	7.450%	80.389%	12.481%	9.777%	T, DiffFSN, NAV, CRC
7.606%	92.394%	7.172%	80.611%	12.299%	9.399%	T, DiffFSN, NAV
7.606%	92.394%	7.348%	80.434%	12.038%	9.322%	T, DiffFSN, CRC
6.658%	93.342%	6.616%	81.041%	11.743%	8.498%	$\Delta Time, T, DiffFSN, NAV$
6.658%	93.342%	7.532%	80.126%	10.465%	8.138%	$\Delta Time, T, DiffFSN, CRC$
6.228%	93.772%	6.514%	81.086%	11.223%	8.011%	$\Delta Time, T, DiffFSN$
4.045%	95.955%	7.120%	80.192%	6.987%	5.124%	T,DiffFSN

Table 4.13 Results for IEEE 802.11 Scenario 10 with SW=20

Scenario 11

This scenario replaces the use of UDP as transport protocol, to force the establishment of TCP sessions prior to sharing any data between AP and client node. In a first sigh to the results, the change introduce has a direct impact in most of the combinations, triggering the FNR to its highest value in most cases. Only the first 6 combinations of the table 4.14 are able to detect the attack with 100% DR.

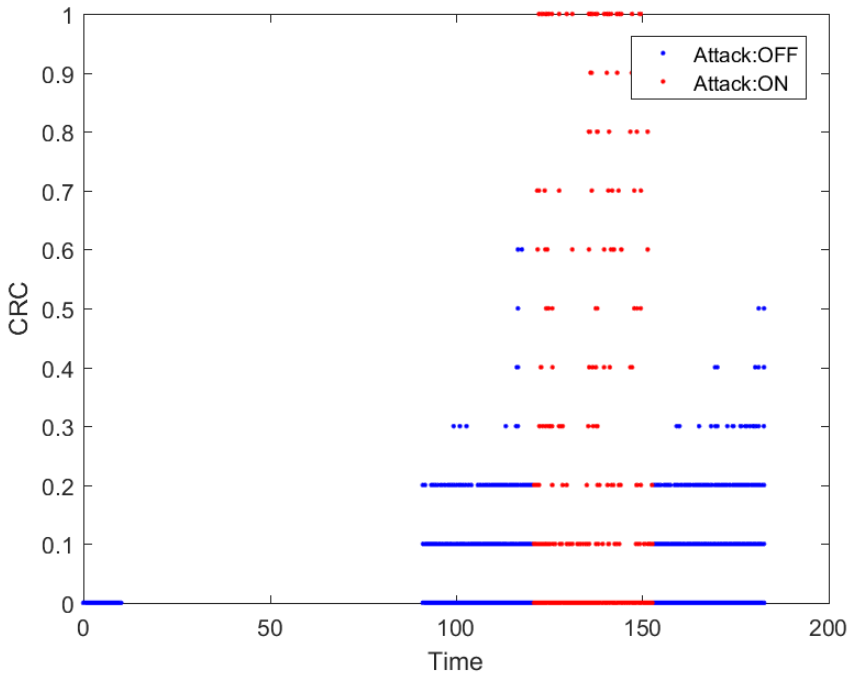


Fig. 4.47 Metric for IEEE802.11 Scenario 11 - CRC

If a threshold is set in the accuracy of the detection performance, only the NAV and (NAV, CRC) metric combinations are able to produce an acceptable Precision and OSR, which is supported by a F_1-Score higher than 80%.

The CRC metric obtains the worse results, with a 100% FNR and 0% DR, registering the measurements depicted in figure 4.47.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	4.528%	95.472%	72.999%	84.392%	NAV
100.000%	0.000%	4.528%	95.472%	72.999%	84.392%	NAV, CRC
100.000%	0.000%	85.526%	14.473%	12.521%	22.255%	$\Delta Time$
100.000%	0.000%	85.526%	14.473%	12.521%	22.255%	$\Delta Time, NAV$
100.000%	0.000%	85.526%	14.473%	12.521%	22.255%	$\Delta Time, CRC$
100.000%	0.000%	85.526%	14.473%	12.521%	22.255%	$\Delta Time, NAV, CRC$
0.580%	99.420%	10.591%	77.238%	0.666%	0.620%	$\Delta Time, DiffFSN, NAV$
0.580%	99.420%	10.591%	77.238%	0.666%	0.620%	$\Delta Time, DiffFSN, NAV, CRC$
0.348%	99.652%	5.777%	82.024%	0.732%	0.472%	DiffFSN, NAV
0.348%	99.652%	5.777%	82.024%	0.732%	0.472%	DiffFSN, NAV, CRC
0.348%	99.652%	10.309%	77.492%	0.411%	0.377%	$\Delta Time, DiffFSN$
0.348%	99.652%	10.309%	77.492%	0.411%	0.377%	$\Delta Time, DiffFSN, CRC$
0.332%	99.668%	5.764%	82.035%	0.700%	0.450%	DiffFSN
0.332%	99.668%	5.764%	82.035%	0.700%	0.450%	DiffFSN, CRC
0.188%	99.812%	0.725%	87.057%	3.078%	0.354%	$\Delta Time, T, DiffFSN, NAV$
0.188%	99.812%	0.725%	87.057%	3.078%	0.354%	$\Delta Time, T, DiffFSN, NAV, CRC$
0.168%	99.832%	0.418%	87.361%	4.688%	0.324%	T, DiffFSN, NAV
0.168%	99.832%	0.418%	87.361%	4.688%	0.324%	T, DiffFSN, NAV, CRC
0.168%	99.832%	0.658%	87.121%	3.030%	0.318%	$\Delta Time, T, DiffFSN$
0.168%	99.832%	0.658%	87.121%	3.030%	0.318%	$\Delta Time, T, DiffFSN, CRC$
0.112%	99.888%	7.249%	80.523%	0.189%	0.141%	T, NAV
0.112%	99.888%	7.249%	80.523%	0.189%	0.141%	T, NAV, CRC
0.112%	99.888%	16.634%	71.138%	0.082%	0.095%	$\Delta Time, T$
0.112%	99.888%	16.634%	71.138%	0.082%	0.095%	$\Delta Time, T, NAV$
0.112%	99.888%	16.634%	71.138%	0.082%	0.095%	$\Delta Time, T, CRC$
0.112%	99.888%	16.634%	71.138%	0.082%	0.095%	$\Delta Time, T, NAV, CRC$
0.036%	99.964%	0.372%	87.391%	1.172%	0.070%	T,DiffFSN
0.036%	99.964%	0.372%	87.391%	1.172%	0.070%	T, DiffFSN, CRC
0.036%	99.964%	5.322%	82.441%	0.083%	0.050%	T
0.036%	99.964%	5.322%	82.441%	0.083%	0.050%	T, CRC
0.000%	100.000%	2.222%	85.536%	0.000%	0.000%	CRC

Table 4.14 Results for IEEE 802.11 Scenario 11 with SW=20

Scenario 12

The last scenario represented on the dataset presents the same characteristics as Scenario 11, increasing the distance between AP and active client host by 5 times. The detection performance shows a satisfactory improvement among all the metric combinations evaluated.

The biggest improvement is produced in the CRC metric, reporting a 100% DR with ∼13.19% Precision caused by the errors reported on the FPR, which has a value of ∼82.25%. The graphical representation of the collected metric values through the duration of the experiment reveal a clean pattern, which is represented in figure 4.48, is the main cause of the massive improvement experienced by this metric.

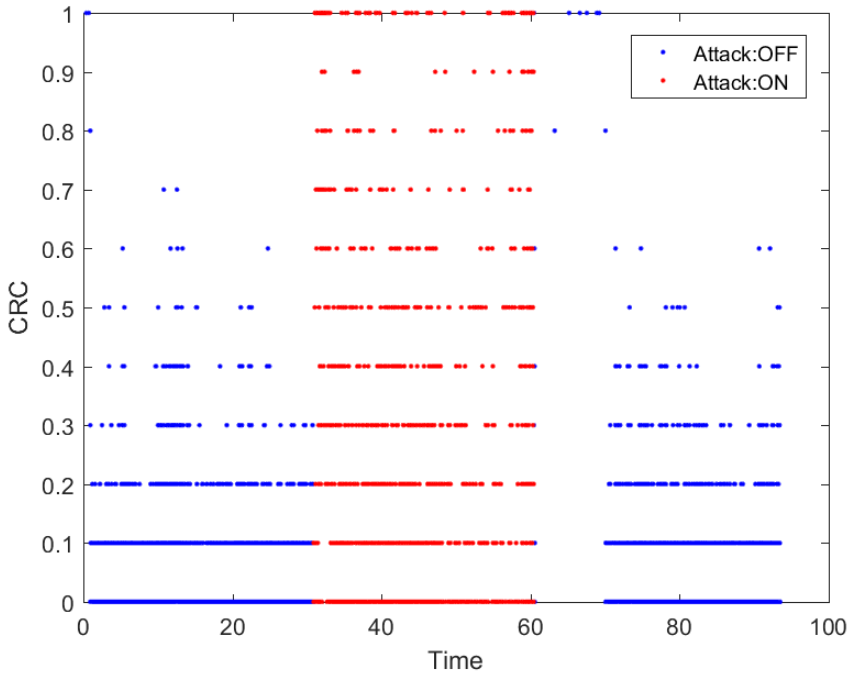


Fig. 4.48 Metric for IEEE802.11 Scenario 12 - CRC

The increase on the distance between the AP and the client causes a natural increase in the CRC errors registered. Since the TCP implement its own mechanism for detecting data frames discarded in transmission in both directions, it also increases the number of data frames required to transmit the same information. Due to that, the probability of CRC errors during the attacking phase is higher, converting this metric in an important indicator to identify the attack.

The rest of the other metrics remains offering a very similar detection performance with a minimal improvement with regard to the analysis described in section 4.4.3.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	5.715%	94.285%	68.612%	81.384%	NAV
100.000%	0.000%	81.449%	18.552%	13.299%	23.475%	$\Delta Time$
100.000%	0.000%	81.449%	18.552%	13.299%	23.475%	$\Delta Time, NAV$
100.000%	0.000%	81.449%	18.552%	13.299%	23.475%	$\Delta Time, CRC$
100.000%	0.000%	81.449%	18.552%	13.299%	23.475%	$\Delta Time, NAV, CRC$
100.000%	0.000%	82.245%	17.755%	13.187%	23.301%	CRC
100.000%	0.000%	82.245%	17.755%	13.187%	23.301%	NAV, CRC
68.469%	31.531%	26.592%	69.469%	24.338%	35.911%	$\Delta Time, T, NAV, CRC$
3.136%	96.864%	20.065%	67.834%	1.915%	2.378%	$\Delta Time, T, NAV$
3.136%	96.864%	20.065%	67.834%	1.915%	2.378%	T, NAV, CRC
3.136%	96.864%	26.099%	61.800%	1.479%	2.010%	$\Delta Time, T, CRC$
1.865%	98.135%	5.946%	81.795%	3.771%	2.496%	$\Delta Time, DiffFSN, NAV, CRC$
1.651%	98.349%	3.620%	84.093%	5.389%	2.527%	$\Delta Time, DiffFSN, NAV$
1.651%	98.349%	3.643%	84.070%	5.356%	2.523%	DiffFSN, NAV, CRC
1.651%	98.349%	5.888%	81.825%	3.383%	2.219%	$\Delta Time, DiffFSN, CRC$
1.469%	98.531%	1.760%	85.931%	9.441%	2.542%	DiffFSN, NAV
1.469%	98.531%	3.617%	84.075%	4.829%	2.253%	$\Delta Time, DiffFSN$
1.469%	98.531%	3.640%	84.051%	4.800%	2.249%	DiffFSN, CRC
1.122%	98.878%	1.759%	85.889%	7.383%	1.949%	DiffFSN
0.880%	99.120%	2.749%	84.868%	3.846%	1.433%	$\Delta Time, T, DiffFSN, NAV, CRC$
0.748%	99.252%	1.278%	86.323%	6.817%	1.348%	$\Delta Time, T, DiffFSN, NAV$
0.748%	99.252%	1.278%	86.323%	6.817%	1.348%	T, DiffFSN, NAV, CRC
0.748%	99.252%	1.802%	85.799%	4.931%	1.299%	$\Delta Time, T, DiffFSN, CRC$
0.242%	99.758%	17.036%	70.501%	0.177%	0.205%	T, NAV
0.242%	99.758%	19.093%	68.445%	0.158%	0.191%	$\Delta Time, T$
0.242%	99.758%	19.093%	68.445%	0.158%	0.191%	T, CRC
0.066%	99.934%	0.962%	86.554%	0.850%	0.123%	T, DiffFSN, NAV
0.066%	99.934%	1.147%	86.369%	0.714%	0.121%	$\Delta Time, T, DiffFSN$
0.066%	99.934%	1.147%	86.369%	0.714%	0.121%	T, DiffFSN, CRC
0.055%	99.945%	16.682%	70.833%	0.041%	0.047%	T
0.022%	99.978%	0.909%	86.601%	0.301%	0.041%	T,DiffFSN

Table 4.15 Results for IEEE 802.11 Scenario 12 with SW=20

4.4.4 LTE Results

The results obtained for the LTE test-bed provide enough evidence to confirm the effectiveness of the proposed metrics on detecting the attack. All the metric combinations evaluated provide an accurate detection performance and reasonable FPR/FNR values, indicating the suitability of the proposed metrics for characterising the DoS Signalling attack studied on this thesis.

Although the metrics have only been evaluated in three scenarios, the strong accuracy of the results obtained makes the detection algorithm an efficient and lightweight on-line IDS able to be implemented in a real 4G deployment.

Scenario 1

The first scenario is the most simple one, with a small duration and equal number of legitimate and rogue UEs. Table 4.16 shows a summary of the detection performance obtained for every possible combination of the three metrics, revealing a fantastic performance.

The highest DR is obtained when using the *Connection Release Rate* (CRR) metric individually, with a 98.1% DR and minimal detection errors, represented on the 1.91% FNR and 11.53% FPR. The detection failures affect negatively to the OSR parameter, due to the impact of the FN and FP cases, but the F_1-Score remains above 90%.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
98.095%	1.905%	11.526%	87.227%	84.774%	90.949%	CRR
97.143%	2.857%	23.988%	74.143%	72.598%	83.096%	CRR, SMT
96.190%	3.810%	0.000%	97.508%	100.000%	98.058%	CRR, SR
88.571%	11.429%	11.526%	80.997%	83.408%	85.912%	CRR, SMT, SR
84.762%	15.238%	23.988%	66.044%	69.804%	76.559%	SMT
83.810%	16.190%	0.000%	89.408%	100.000%	91.192%	SR
82.857%	17.143%	0.000%	88.785%	100.000%	90.625%	SMT, SR

Table 4.16 Results for LTE Scenario 1 with SW=20

In section 4.4.1, when defining the performance indicators, it was stated that the DR by itself does not provide an accurate view of the overall detection performance on each case. This affirmation becomes more obvious if the results obtained are analysed for the following metric combinations: (CRR, SR) and SR (*Success Rate*); where the DR is lower than the top metric combination (CRR), but has a higher OSR, Precision and F_1-Score. In contrast, the (SMT, SR) combination metric also achieves a lower DR, registering a higher SR and Precision, but is

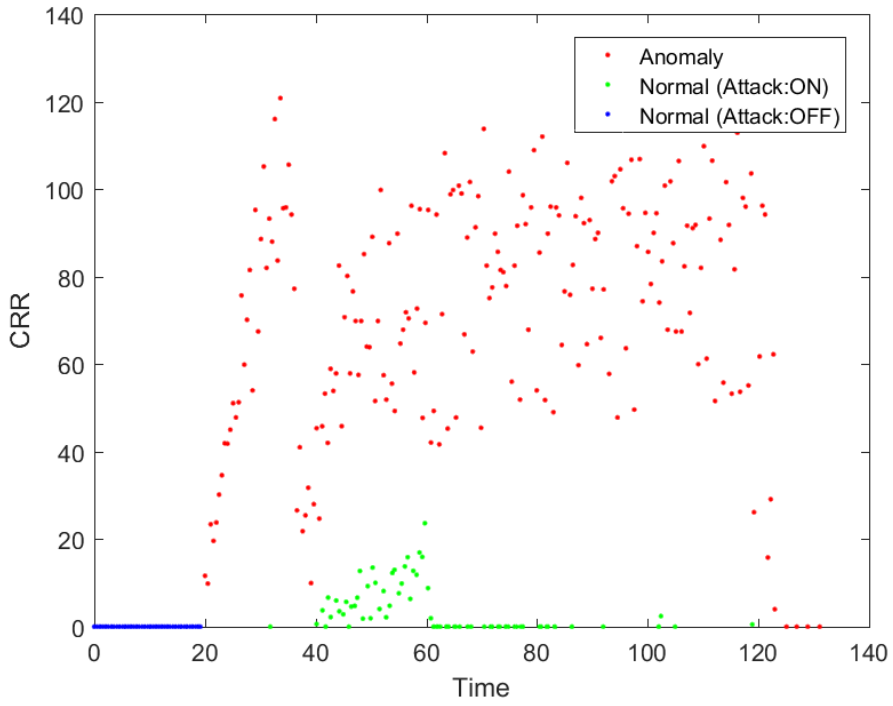


Fig. 4.49 Metric for LTE Scenario 1 - CRR

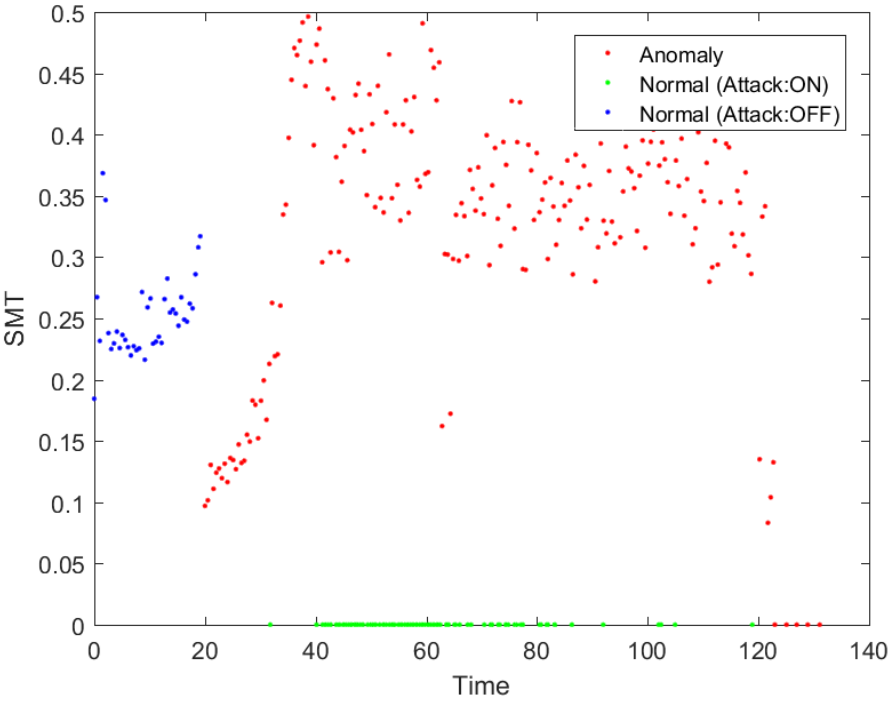


Fig. 4.50 Metric for LTE Scenario 1 - SMT

unable to overpass its F_1-Score value due to the important difference in DR caused by a lower number of TP cases.

Looking at the representation of each metric in figure 4.49, figure 4.50 and figure 4.51, it is possible to differentiate the exact moment when the attack is triggered and its effect on the metric values.

The results obtained on the scenario 1 are displayed on the following figure 4.49, figure 4.50 and figure 4.51.

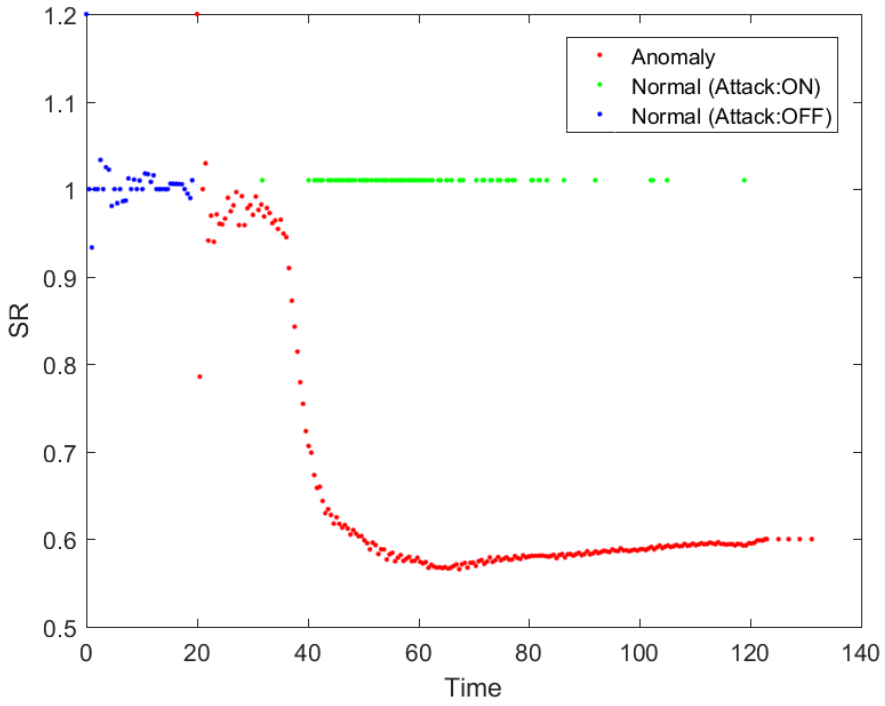


Fig. 4.51 Metric for LTE Scenario 1 - SR

Scenario 2

Combining the metrics (CRR, SR), the DR is equal to 100%, with an accuracy of 100% registered across all the performance parameters: OSR, Precision and F_1-Score. This is due to the null FP and FN cases registered for this set of metrics, offering the best outcome possible. If the analysis is reduced to the individual evaluation of the CRR metric, the detection performance only decreases less than 2% for the DR and OSR, and ∼0,6% for the F_1-Score indicator.

The positive detection trend obtained on this scenario is due to the changes performed on the definition of Scenario 2. The first variation is an extension of the emulation by more than 12 minutes. Additionally, the ratio of legitimate/rogue UEs is balanced in favour of the rouge UEs

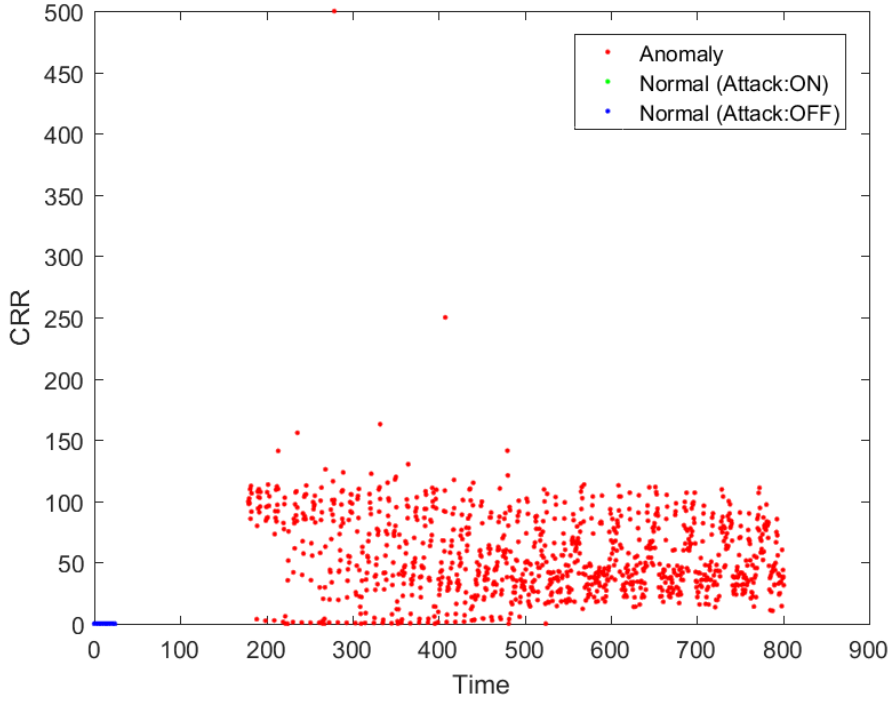


Fig. 4.52 Metric for LTE Scenario 2 - CRR

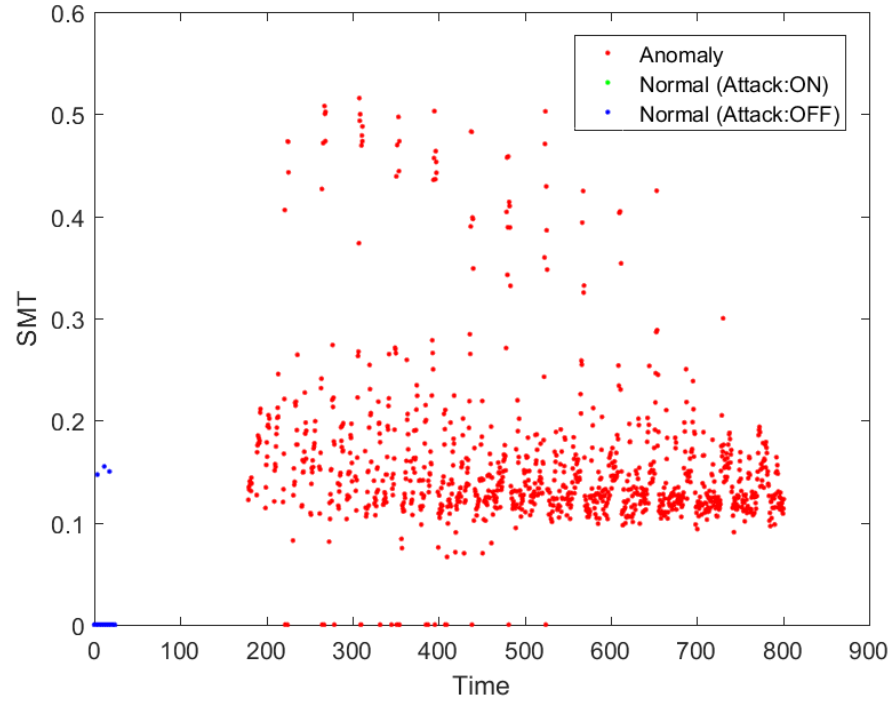


Fig. 4.53 Metric for LTE Scenario 2 - SMT

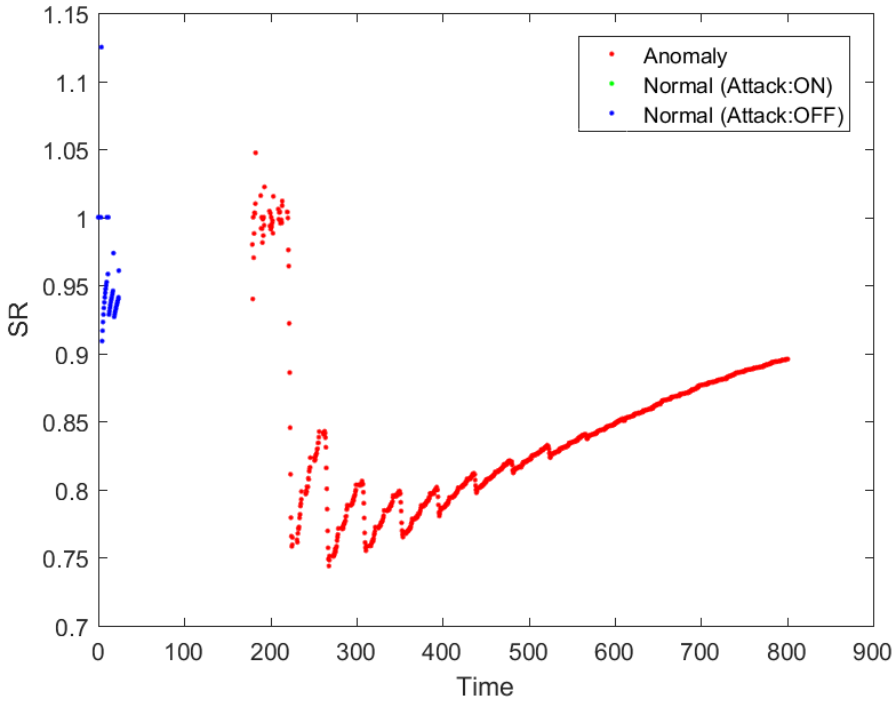


Fig. 4.54 Metric for LTE Scenario 2 - SR

by 9 times. This second change produces a drastic increase on the malicious network traffic, facilitating the construction of the normality and anomaly patterns by the detection algorithm.

The last four metric combinations on table 4.17 have suffered an important increase of ∼10% with regard to the DR values registered on the previous Scenario 1.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
100.000%	0.000%	0.000%	100.000%	100.000%	100.000%	CRR, SR
98.814%	1.186%	0.000%	98.862%	100.000%	99.403%	CRR
97.536%	2.464%	0.088%	97.548%	99.907%	98.707%	SMT
97.536%	2.464%	0.088%	97.548%	99.907%	98.707%	CRR, SMT
97.536%	2.464%	0.088%	97.548%	99.907%	98.707%	CRR, SMT, SR
96.989%	3.011%	0.088%	97.023%	99.906%	98.426%	SMT, SR
95.803%	4.197%	0.000%	95.972%	100.000%	97.857%	SR

Table 4.17 Results for LTE Scenario 2 with SW=20

If the values registered on each metric are analysed by looking at the figures, a more abrupt increase occurs in the exact moment the attack is launched, enabling the rogue UEs which start injecting malicious traffic on the core network.

Scenario 3

Finally, the last Scenario to be evaluated for the LTE experiments uses the same configuration as the previously analysed Scenario 1. However, the total duration of the emulation has been extended more than 6 times the initial duration. The wider duration affects not only to the initial/attack phase, but also to the final phase.

In general, the changes produce a positive effect in the registered DR values across all the metrics. A significant increase of the FNR and FPR is detected for better performing metric combinations, reaching up to 0.1% and 1.92% in the worse cases, respectively.

The CRR metric outperforms in all the metric combinations where it is used, having its best performance when used individually with a ∼99.92% DR and an extremely positive accuracy across all the cases. The F_1-Score remains close to 100%, with a distance lower than 2%.

DR	FNR	FPR	OSR	Precision	F_1-Score	Metrics
99.915%	0.085%	1.918%	98.011%	97.765%	98.828%	CRR
99.915%	0.085%	1.918%	98.011%	97.765%	98.828%	CRR, SR
93.401%	6.599%	0.852%	93.608%	98.925%	96.084%	SMT
93.401%	6.599%	0.852%	93.608%	98.925%	96.084%	CRR, SMT
93.401%	6.599%	0.852%	93.608%	98.925%	96.084%	CRR, SMT, SR
79.272%	20.728%	0.852%	81.747%	98.736%	87.940%	SMT, SR
0.423%	99.577%	0.000%	16.406%	100.000%	0.842%	SR

Table 4.18 Results for LTE Scenario 3 with SW=20

However, the worst performance detection registered for the entire dataset is produced when using the SR metric individually. The DR drops to ∼0.42%, the lowest value registered for the attack with the proposed detection algorithm. To better understand the reason why this metric becomes misleading, producing a ∼99.58% FNR and an OSR value of ∼16.41%, all the values collected on this scenario have been represented in figure 4.55, being difficult to identify a clear pattern on the represented values.

The SR measures the average ratio of successful RRC session established by each node, which makes this metric less volatile over long period of evaluation. This is due to the fact that

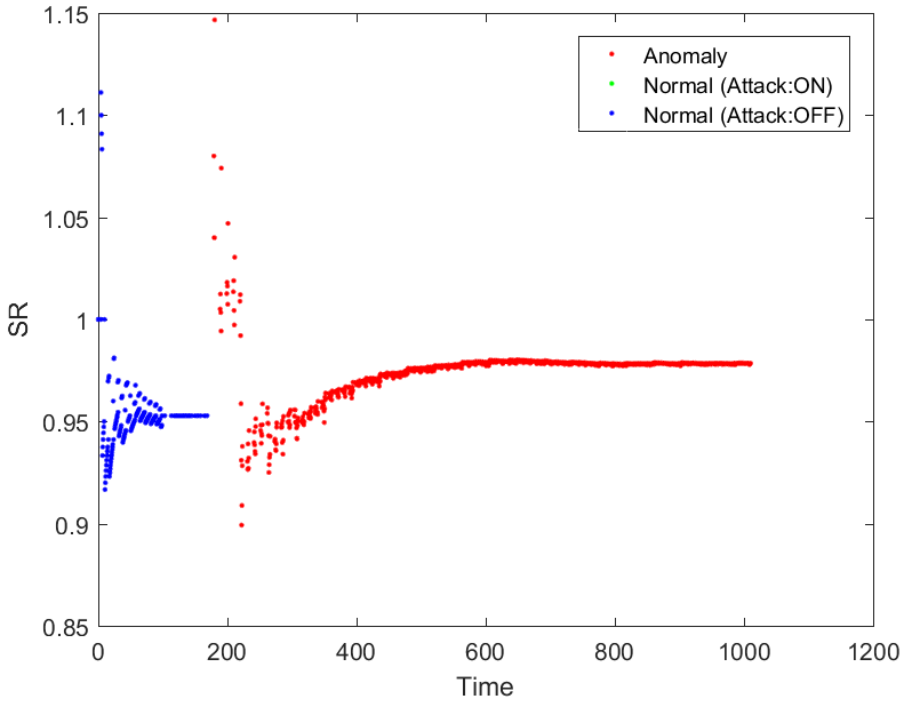


Fig. 4.55 Metric for LTE Scenario 3 - SR

every UE will only establish a new RRC session if it has migrated from RRC-CONNECTED to RRC-IDLE for any of the reasons describe in Chapter 2.

Nevertheless, this metric remains being very useful to detect the RRC signalling attack studied on this thesis, as it does not increase the FPR when combined with the CRR while still offering a very high DR and OSR values. Moreover, the combination of multiple metrics in the detection algorithm makes the final IDS more robust and resilient against abrupt changes in the network traffic behaviour.

4.5 Summary

This chapter has detailed all the challenges faced for designing, obtaining the required equipment, configuring it and finally utilising it to build the test-beds required for producing a dataset for LTE and WiFi networks. The network traffic gathered on each dataset contains traces of anomaly traffic generated while performing a virtual jamming attack on IEEE 802.11 networks, and a RRC signalling attach on LTE networks, which are the main area of study chosen for this thesis.

A complete range of traffic patterns have been presented and included on the dataset, inspired by real-life scenarios where special cases are considered to guarantee a better characterisation of the attacks. Finally, an exhaustive analysis of all the results is presented, including a list of figures on each scenario to better understand the complexity faced by the detection algorithm and how it adjusts itself to maintain an optimal detection performance.

The results studied on this chapter support the effectiveness of the new metrics proposed on this thesis. The NAV metric provides the best overall detection performance for IEEE 802.11 technologies, strengthening the detection algorithm against unexpected changes on the normal network traffic pattern when it is combined with two additional metrics: CRC and/or Δ Time.

Finally, the results obtained for the LTE test-bed revealed the CRR metric as the most effective for detecting the RRC signalling attack, registering a strong detection performance when used individually or in combination with the *Session Mean Time* (SMT) and *Success Rate* (SR) metrics.

CHAPTER 5

Conclusions and future work

This chapter closes the thesis with a brief interpretation of the research findings obtained while conducting this research project, with special focus on the most productive phases in term of outcomes: the experimental and analysis phases. Section 5.1 performs an empirical analysis of the results collected in the two test-beds, extracting the most valuable conclusions and deducted achievements. A special emphasis is placed on the new set of metrics identified as effective indicators for detecting DoS attacks in wireless and cellular networks, which has been experimentally tested and successfully evaluated.

Section 5.2 presents a clear explanation of the experimental method followed on this thesis to validate the collected results and deduct the conclusions, confirming the applicability in any real network.

The validation method is followed with a synthesised description of the most important contributions of this work, which are presented in section 5.3. In addition, this section sums up the multiple actions taken to disseminate the research findings, and exposing them to peer-reviewing analysis. The list includes all the research events, conferences and journals where this work has been published and shared with the research community, without excluding the local academic events attended as student at Loughborough University.

Lastly, additional ideas are presented in section 5.4 for extending this work, aiming at overcoming the existing limitations and extending the scope of this research direction to address the existing challenges.

5.1 Conclusions

This thesis has successfully discovered a new method for identifying *Denial-of-Service* (DoS) attacks in radio-based communication systems. The proposed algorithm can be easily implemented into an *Intrusion Detection System* (IDS) without adding much computational load to it. The mathematical operations required on each iteration of the sliding window are basic operations, providing an overall low computational complexity to complete the detection process with the fusion of beliefs.

The proposed solution extracts meaningful information from every frame for the suggested metrics, as part of the sample collection process, eliminating the need of temporary storing all the data transferred through the communication channel. The collected results reveal a variation of the effectiveness for each metric combination depending on the conditions of the network, which can be used to tailor the algorithm for an specific network usage pattern.

Using a single metric, both DoS attacks have been successfully detected with *Detection Rate* (DR) higher than 90%. In the same line, the *Overall Successful Rate* (OSR) remains above 75% for 11 of the 12 scenarios evaluated for *Wireless Fidelity* (Wi-Fi), and the totality of the scenarios evaluated for the *Long Term Evolution* (LTE) attack. The satisfactory results registered demonstrate the effectiveness of the proposed metrics to characterise the targeted DoS attacks. This characteristic makes the detection algorithm fully compatible with IDS implementations for the future *multi-Radio-Access Technologies* (multi-RAT) cellular networks[84], where WiFi and LTE are expected to be the two major standards for accessing Internet [5].

The design of three new metrics for the DoS attack in LTE networks has been a real challenge, due to the lack of previous work conducted within the research community to set the state of the art. The results obtained with the LTE emulated environment have been very satisfactory, registering only two metric combinations where the detection algorithm was not able to correctly identify the attack. For all the other cases, the DR remains above 80% with OSR values higher than 80%, or almost close to 100% in most of the cases.

5.1.1 IEEE 802.11 virtual jamming attack

The first conclusion obtained after analysing the data-set becomes obvious when looking at the collected results. The effectiveness of the NAV metric provides a quasi-perfect detection performance, reaching 100% in all the cases whenever this metric is individually used on the detection algorithm. Since the implementation of the attack sets a fixed value on the NAV field within the MAC message header, this parameter becomes very sensitive for detecting the attack.

The lowest *False Positive Rate* (FPR) registered across all the experiments is detected when individually using the NAV metric to detect the attack on Scenario 3, where only a single active

node in motion is sending traffic through the *Access Point* (AP). This is a clear indicator of how positively the NAV metric adapts to constant changes in the radio parameters due to the node's movement.

Nevertheless, it is important to remember that defining the NAV field to its maximum value is not a clear indicator of rogue behaviour by itself. The use of the NAV metric must be strengthened with additional metrics to reduce the FPR in congested wireless networks, where fragmentation on the data frames increases the number of messages with high NAV field values [30]. Having high values in the NAV field causes the legitimate nodes to register a similar pattern to traffic coming from the jammer node, the attacker. Since the proposed NAV metric looks at the mismatching between the duration indicated on the NAV field, and the actual duration of the transmitted frame, evaluating long periods of transmissions with fragmented frames could affect the attack detection effectiveness when using only the NAV metric.

The Δ Time metric has also obtained very high detection performance in all the Wi-Fi scenarios, evaluating a DR lower than 75% in a single scenario, Scenario 8, where the DR falls to $\sim$66%. This decrease is directly caused by the existence of a node using *Request-To-Send/Clear-To-Send* (RTS/CTS) mechanism while located in a fixed position close to the AP. This node registers a small frame inter-arrival time due to the short distance to the AP, registering also minimal frame discarding due to collisions thanks to the RTS/CTS mechanism, which produces a Δ Time value similar to the attacker. Fortunately, the lack of clarity when used individually can be reduced by combining this metric with NAV, boosting the DR to $\sim$83.71% while maintaining the OSR around $\sim$43.20%. The metric combination (Δ Time, CRC) and (Δ Time, NAV, CRC) achieve the same DR, registering a higher FPR that reduces the OSR down to $\sim$36.74%.

The outstanding performance obtained by the Δ Time metric in Scenario 11 and 12, where the DR is equal to 100% and the False Negative (FN) are reduced to 0%, reveals the effectiveness of this metric for detecting the attack in networks with predominant *Transmission Control Protocol* (TCP) traffic. This transport protocol increases the number of packets exchanged between nodes due to the additional traffic load imposed by the TCP mechanisms. This protocol requires of a constant control message for establishing the connection, maintaining the link alive, acknowledging the received messages and/or requesting re-transmissions when needed. On the contrary, this metric is also prone to producing high *False Positive* (FP) alarms, registering values above 50% across all the scenarios when being evaluated individually.

The following conclusion to highlight is obtained when analysing the behaviour of the CRC metric on the 12 scenarios studied, proving itself not adequate in wireless networks where the number of active nodes is small, and they are not in motion. These two factors facilitate the availability of the communication channel, reducing to the minimum the probabilities

of suffering collisions in a radio channel with stable parameters. The CRC metric produced extreme results, detecting all the *True Positive* (TP) cases with a DR of 100% and 0% *False Negative Rate* (FNR) in 7 scenarios (Scenario 3, 5, 6, 8, 9, 10 and 12), or 0% DR and 100% FNR in the remaining 5 scenarios.

Moreover, the perfect DR values come at the price of reducing the accuracy of the overall detection, with an OSR ranging from 31.15% to 17.76%, and an average FPR of 77% across the 7 scenarios where the attacker's frames were successfully detected. Furthermore, if the (CRC, NAV) metric combination is analysed on the seven positive scenarios mentioned before, the CRC metric only adds value in Scenario 9, helping to reduce the FPR by $\sim$46.2% and consequently boosting the OSR by $\sim$46.8% while maintaining the 100% DR.

The last two metrics to analyse for extracting valuable conclusions are DiffFSN and T. These two metrics does not provide enough evidence of the attack by themselves, requiring a fuse of intelligence coming from other metrics to provide an acceptable DR.

The DiffFSN metric fails to detect the attacker's frames, reaching a maximum 36% DR with a high OSR of 80% in Scenario 6. However, the Precision is extremely low, with a basic $\sim$7.58%, which pushes the F_1-Score down to $\sim$12.55%. This metric obtains its best results when using UDP traffic, as it doesn't produce any frame retransmission that could increase the time between two consecutive frames successfully delivered. Any attacker frame missed on reception due to the collisions will cause a slightly increase on the samples collected by this metric, facilitating the registered TP value. Furthermore, it will also increase the chances of FP whenever the collisions occur as part of the traffic exchanged between the legitimate nodes, or due to the hidden node phenomenon.

Combining the DiffFSN metric with any of the other 4 metrics does not provide any better detection performance in most of the scenarios, obtaining a minimal increase in Scenario 2, 8, 9, 10, 11 and 12, when this metric is combined. The best increase is up to 12% on the DR in Scenario 2, when this metric is used in combination with Δ Time and NAV, registering the forth best DR on this scenario, and the second best OSR with $\sim$68.04%.

If the DiffFSN metric is combined with (Δ Time, NAV, T, CRC), (Δ Time, NAV, CRC), (Δ Time, T, NAV) or (NAV, CRC), the DR suffers an increase up to $\sim$2%, with respect to the rest of the metric combinations including the DiffFSN.

Scenario 2 has proven to be the most challenging experiment conducted, due to its simplicity. The two active nodes only transfer UDP data-frames, which no protection against collisions or missed packages. Furthermore, the distance between them is long enough to produce some collisions due to the hidden node problem. However, the absence of motion helps the DiffFSN metric to quickly build the normality pattern and easily differentiate it from the changes inflicted

on the network traffic pattern by the attacker. The same occurs with the Δ Time metric on this scenario, positioning itself as the second best metric right after the NAV metric.

Finally, the analysis of the results obtained for the T metric provides evidence of the value added when it is combined with other metrics. It obtains its best DR when combined with the NAV and CRC metrics on Scenario 10, reaching a DR of ∼71.7% with an OSR of ∼53.44%, although it only provides a reduced F_1-Score of ∼28.94% due to the high FPR, which is ∼2.82%.

The T metric becomes more sensitive to variations whenever there are active nodes located far from the AP, such as in Scenario 10, 7 and 12, where the DR is above 67.05% for all the metric combinations which includes the T metric. Longer distances increase the chances of suffering reflections on the radio bearer due to objects between the node and the AP, forcing the throughput to fluctuate depending on the signal quality registered on the radio link. However, the best result for the individual use of the T metric is registered in Scenario 7, with a ∼67.05% DR. On this case, the OSR decreases to ∼55.47% due to the more than 30% value obtained for the FPR and value registered for the FNR.

Scenario 7 is composed by a single static node, which produces a constant network traffic flow due to the RTS/CTS mechanism, stabilising the throughput. When the attack is triggered, it causes an abrupt change on the T metric, which disappears after a few seconds once the throughput has been stabilised down to 0%. It is only during the abrupt changes when this metrics obtains its best performance.

To conclude, the experiments conducted on this thesis can be used to affirm that the metrics proposed are able to detect the attack in all the scenarios. In particular, the NAV metric has proven to be the most meaningful metric to characterise the attack across all the evaluated scenarios, followed by the Δ Time and CRC metrics. The best metric combinations to provide an overall detection performance in most of the scenarios are: (Δ Time, NAV) and (NAV, CRC). These two metric combinations are the ideal candidates to be implemented into an IDS system without requiring any additional knowledge of the targeted wireless network.

5.1.2 LTE signalling attack

The LTE experiments have proven how accurately the proposed metrics detect the attack, no matter if they are used individually or as part of a set of metrics. However, if the individual performance of each metric is analysed, the *Connection Release Rate* (CRR) metric raises as the strongest metric to detect the attack, with a DR higher than 98% in the three scenarios presented on this thesis. This conclusion was predictable due to the fact that the process for performing the DoS attack studied on this thesis is by creating an unusual traffic of *Radio Resource Control* (RRC) Connection Request, which might end up with a RRC Connection

Release message when the attacker's requests are rejected, or in specific legitimate cases as mentioned in Chapter 3.

The best overall performance is obtained in Scenario 2, with the metric combination (CRR, SR), when every single frame is correctly tagged and all the performance indicators reach their highest positive value. The DR and OSR are raised to 100%, due to a very accurate detection with a Precision and F_1-Score of 100%. This result is specially important because Scenario 2 was specifically designed to facilitate the detection, with only 50 legitimate *User Equipments* (UEs) and 5 times more rogue UEs.

If the same metric combination is evaluated in the Scenario 1 and 3, where the legitimate/rogue UE ratio is equal to 1, the DR decreases down to 96.19% when the emulation duration is short, or ∼99.92% when the experiment has a duration similar to Scenario 2. In both cases, the OSR and F_1-Score obtain very positive results, remaining above 97.5% due to the accuracy on the classification of the collected network traffic.

The *Session Mean Time* (SMT) metric is the second metric providing the best results, requiring a long duration of the emulation to guarantee the best performance. This metric is able to detect the attack with a DR of ∼97.54% and ∼93.4% in Scenario 2 and 3, respectively. On the contrary, the OSR obtains a better result in Scenario 2, with a ∼97.55% against the ∼93.62% evaluated for Scenario 3 due to the increase of FNR, with a ∼6.6%. The reason for this minor difference is one more time the ratio between legitimate and rogue UEs, as only the legitimate UEs are able to successfully complete an RRC session and modify the average RRC session aliveness monitored by the SMT metric.

If the behaviour of the SMT metric is analysed when it is combined with either the *Success Rate* (SR) or the CRR metrics, it is possible to perceive an important decrease of the DR and increase on the FNR. Scenario 1 registers the worse case, when the (SMT, SR) metric combination manages to obtain a decent 82.86% DR. This value implies a reduction of almost 15% on the DR if it is evaluated against its highest detection performance, when this metric is individually used in Scenario 2. However, even in this case, this metric combination is able to provide a high level of accuracy, with a 100% Precision and F_1-Score of 90.63%

The lowest result across all the conducted experiments is registered for the SR metric in Scenario 3, with an unacceptable ∼0.42% DR and FNR of ∼00.58%. The registered Precision is 100% due to the absence of FP cases, which boosts the OSR to a minimal ∼16.41%.

Although the SR is present in all the lowest DR registered on all the scenarios, it adds value when combined with the CRR metric, as previously mentioned at the beginning of this section. The (CRR, SR) metric combination provides positive results not only for aforementioned Scenario 2, but also in the remaining experiments, as introduced before. It obtains a DR higher

than 96% in both scenarios, which is backed up with an OSR of 97.51% in Scenario 1, and a better 98.01% OSR in Scenario 3.

Looking at the obtained results, it is possible to conclude that an attacker attempting to execute the signalling DoS attack should inject a similar number of RRC Connection Request messages equivalent to the actual number of legitimate requests registered on the network, reducing the attack duration to short periods of time. The optimisation of the attack implies a period of monitoring the channel, in an attempt to match the average legitimate RRC Connection Request messages registered within a certain time. Only by tailoring the attack duration and injection rate, the attacker will be able to reduce the chances of being detected by the proposed algorithm.

5.2 Validation Methodology

The process to validate the proposed detection algorithm is based on the experimental evaluation of its detection performance against a test battery of real scenarios. This process was followed for every candidate metric deduced during the analysis and characterisation of the DoS attacks. Due to that reason, the attack characterisation and definition of candidate metrics have been included as steps of the validation methodology.

During the creation of the scenarios for Wi-Fi and LTE technologies, the author of this thesis focused on selecting realistic episodes of real-life usage patterns. Additionally, edge cases where added to the test battery, where the detection process was expected to have a poor performance due to the direct effects on the variables included to calculate the selected metrics.

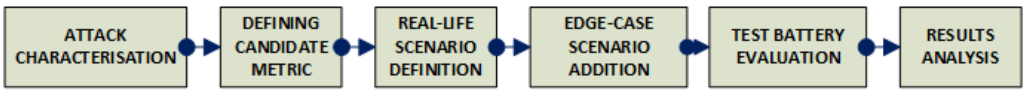


Fig. 5.1 Steps of the Validation Methodology

Figure 5.1 represents the validation approach followed on this thesis to confirm the effectiveness of the detection algorithm, and the suitability of the proposed metrics to detect the two DoS attacks. Although the results obtained are directly affected by the selected thresholds when assigning the beliefs in Normal/Attack and the *Sliding Window* (SW) size, they are an objective and clear evidence of the effectiveness when the algorithm is adjusted to detect specific threats. In Appendix A, additional results are presented with alternative SW sizes and similar detection results. These results evidence the wide tolerance of the proposed algorithm to be readjusted, and its suitability to be implemented in a generic IDS to detect multiple attacks.

5.3 Contributions

The work conducted during this research project has facilitated the achievement of five major contributions on the study of attacks against the service availability on wireless and cellular networks, as Chapter 1 introduced briefly:

Identidifaction of metrics for detecting DoS attacks in Wi-Fi

This thesis has presented and evaluated the effectiveness of a new set of metrics able to characterise virtual jamming attacks in *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 networks. The proposed metrics have been tested against multiple scenarios and network traffic patterns, individually and as part of a subset, providing positive, reliable and accurate detection results for all the cases analysed on the dataset.

Design of a test-bed to perform virtual jamming attacks on Wi-Fi networks

Combining equipment with basic hardware specifications, equivalent to any device available in the market for domestic use, this thesis has created a test-bed and successfully implemented a virtual jamming attack. The implementation of the attack exploits the CTS/RTS mechanism and the procedure for computing the back-off time on each node using the NAV field.

Creation of three new metrics for DoS attacks in LTE

Due to the lack of existing work conducted by other researchers, this thesis conducted a new characterisation of the RRC signalling attack with the purpose of finding meaningful metrics. The proposed three metrics, CRR, SE and SSR, have been experimentally validated, obtaining a satisfactory detection performance not only when used individually, but also when they are combined as part of a set of metrics.

Emulation of RRC signalling attack in LTE

Using the test-bed proposed on this thesis, composed of LTE emulation equipment, it was possible to perform the study of the RRC signalling attack. The proposed implementation replicates the conditions of suffering the attack in a commercial LTE deployment. The results, obtained by analysing the network traffic collected on the test-bed, demonstrate how easy the attack can be performed in a matter of minutes.

Novel on-line IDS to detect multiple DoS attacks

The presented detection algorithm meets all the requirements to be implemented in an on-line IDS, offering a fast, efficient and lightweight mechanism for detecting two particular DoS attacks. The implementation of this algorithm into an IDS, which could be embedded into a femtocell device for future 5G networks, could be easily achieved

without affecting the network performance. MNOs could use it as defence mechanisms for protecting their public networks against attacks targeting the service availability, protecting not only their interests but also providing safer communication services to their customers.

5.3.1 Publications

The findings obtained on this thesis has been presented, exposed to open discussion, peer-reviewed and finally published in different conferences and editorials. The following paragraphs enumerate the list of publications resulting from this work, classified by publication type and including the internal publications presented as part of the PhD research degree programme and the research skills development plan.

Conference Proceeding Papers

- [85] G. Escudero-Andreu, Raphael C.-W. Phan and David J. Parish, *Analysis and Design of Security for Next Generation 4G Cellular Networks*, The 13th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNET), 2012.

- [43] G. Escudero-Andreu, K. G. Kyriakopoulos, F. J. Aparicio Navarro, D. J. Parish, D. Santoro and M. Vadursi, *A Data Fusion Technique to Detect Wireless Network Virtual Jamming Attacks*, The IEEE International Workshop on Measurements & Networking (M&N), 2015.

Journal Articles

- [86] D. Santoro, G. Escudero-Andreu, K. G. Kyriakopoulos, F. J. Aparicio Navarro, D. J. Parish and M. Vadursi, *A Hybrid Intrusion Detection System for Virtual Jamming Attacks on Wireless Networks*, Measurement, Elsevier, 2017.

Internal School Publications

- Abstract presented at the annual conference on the School of Electronic, Electrical and Systems Engineering, 2011.

- Poster presented at the annual conference on the School of Electronic, Electrical and Systems Engineering, 2012.

- Poster presented at Loughborough University on the *Research That Matters Conference*, 2013.
- Short paper presented at the annual conference on the School of Electronic, Electrical and Systems Engineering, 2014.

5.4 Future work

To conclude the chapter, this section indicates the main research directions that could help expanding the work conducted on this research project, aiming at improving the obtained detection performance. Looking at the current trends on anomaly detection and wireless network security, the author expresses his opinion on the most suitable ideas for enhancing the contributions of this thesis.

In an attempt to reduce the level of type-I and type-II errors, the metrics proposed on this thesis should be enriched with *contextual information*, as this information has proven very valuable for understanding the results obtained in Chapter 4 on each scenario. Current trends within the research community reveal a notorious interest [87, 88] on applying the knowledge, easily deducted from expected network usage patterns and historical records, as contextual information to be included into the detection phase. The benefits of making the IDS aware of the surrounding network environment have proven very valuable to boost the IDS performance and reduce unnecessary alarms or FP [89, 70, 88].

The second approach to extend this work would focus on discovering additional metrics capable of enhancing the detection performance. IEEE 802.11 was first released in 1997 and has been widely studied over the past few years, reducing the chances of finding new metrics which have not been studied before. However, LTE is a relatively new technology and not much research has been conducted on protecting it against signalling DoS attacks with IDS and anomaly detection techniques.

The metrics presented on this thesis are very efficient to detect the specific attacks studied during this research project. However, LTE networks are exposed to additional threats and further research should be conducted to verify the applicability of the existing metrics to detect other attacks, as well as aiming to reduce the false alarms incorrectly raised when using the proposed metrics.

Furthermore, the results presented on this thesis have been collected after reproducing real-life scenarios, which were designed to cover all the expected user behaviours and problematic edge cases. However, further scenarios should be evaluated against the same metrics to discover alternative metric combinations capable of reproducing the already registered detection results under different network traffic patterns. This idea becomes more interesting for the LTE

experiments, where the test-bed was composed by 3 emulated scenarios due to the legal impediments for evaluating the detection performance in a real LTE deployment.

Finally, this thesis has opened a new research direction towards the actual implementation of the proposed set of metrics into a centralised multi-RAT IDS capable of protecting not only local *Wireless Local Area Networks* (WLANs), but also cellular *Wide Area Networks* (WANs). Using monitoring stations at the endpoint equipment, such as the *evolved-Node B* (eNB) and/or the femtocell units, the hybrid IDS can easily be hosted within the Mobile Network Operator's (MNO) network to prevent any physical tampering and facilitate the management process. However, the IDS design and optimal installation within the cellular network must be first investigated thoroughly to guarantee the best performance while keeping the low computational overhead and manageable data flows.

References

[1] 3GPP TS 36.213, "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures," no. v.14.2.0 - Release 14, pp. 0–6, 2017.

[2] LAN/MAN Standards Committee, *Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band*, vol. 2012. 2012.

[3] Ericsson, "Ericsson Mobility Report," Tech. Rep. June, 2017.

[4] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," in *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005.*, pp. 719–724, jun 2005.

[5] T. J. Barnett, A. Sumits, S. Jain, and U. Andra, "Cisco Visual Networking Index (VNI): Global Mobile Data Traffic Forecast Update, 2016-2021," *Vni*, pp. 1–35, 2017.

[6] The Instant Group, "UK Flexible Workspace Review," tech. rep., 2016.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[8] B. P. Crow, I. Widjaja, L. G. Kim, and P. T. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine*, vol. 35, pp. 116–126, sep 1997.

[9] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, pp. 66–74, apr 2011.

[10] D. Welch and S. Lathrop, "Wireless security threat taxonomy," in *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.*, pp. 76–83, jun 2003.

[11] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions.," in *USENIX security*, pp. 15–28, 2003.

[12] K. Bicakci and B. Tavli, "Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.

[13] C. E. Vintila and V. V. Patriciu, "Security Analysis of LTE Access Network," *ICN 2011, The Tenth International*, no. c, pp. 29–34, 2011.

[14] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating IMSI Catchers," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, (New York, NY, USA), pp. 340–351, ACM, 2015.

[15] R. Borgaonkar, K. Redon, and J.-P. Seifert, "Security analysis of a femtocell device," *Proceedings of the 4th international conference on Security of information and networks - SIN '11*, p. 95, 2011.

[16] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, "LTE for public safety networks," *Communications Magazine, IEEE*, vol. 51, pp. 106–112, feb 2013.

[17] M. Ulema, A. Kaplan, K. Lu, N. Amogh, and B. Kozbe, "Critical communications and public safety networks part 1: Standards, spectrum policy, and economics," *IEEE Communications Magazine*, vol. 54, pp. 12–13, mar 2016.

[18] R. Favraud, A. Apostolaras, N. Nikaein, and T. Korakis, "Toward moving public safety networks," *IEEE Communications Magazine*, vol. 54, pp. 14–20, mar 2016.

[19] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of Wireless Communication Technologies for Public Safety," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 2, pp. 619–641, 2014.

[20] UK Gobernment. Home Office, "Emergency Services Mobile Communication Programme (ESMCP)," 2015.

[21] M. Donahoo and B. Steckler, "Emergency mobile wireless networks," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pp. 2413—-2420 Vol. 4, oct 2005.

[22] B. P. Gautam and K. Wasaki, "Using a redundant Wi-Fi network as an emergency detour route to proactively reduce disaster risk in Wakkanai, Hokkaido," in *2014 International Conference on Information Science, Electronics and Electrical Engineering*, vol. 3, pp. 1830–1837, apr 2014.

[23] UK Legislation, "Communications Act 2003," 2003.

[24] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[25] D. Yu and W. Wen, "Non-access-stratum request attack in E-UTRAN," *Computing, Communications and Applications*, pp. 48–53, 2012.

[26] H. Choudhury, B. Roychoudhury, and D. K. Saikia, "Enhancing User Identity Privacy in LTE," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 949–957, jun 2012.

[27] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[28] L. Wang and A. M. Wyglinski, "A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks," in *Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference on*, pp. 809–814, aug 2011.

[29] D. Chen, J. Deng, and P. K. Varshney, "Protecting Wireless Networks Against a Denial of Service Attack Based on Virtual Jamming," in *ACM MobiCom*, vol. 3, pp. 14–19, 2003.

[30] M. Gast, *802.11 Wireless Networks: The Definitive Guide*. A Nutshell handbook, O'Reilly Media, 2005.

[31] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, New Jersey, USA: Princeton University Press, 1976.

[32] OPNET Technologies Inc., "OPNET Modeler Suite," 2017.

[33] Aeroflex Inc., "Aeroflex E500 Network Tester," 2017.

[34] M. Kim and C. H. Choi, "Hidden-Node Detection in IEEE 802.11n Wireless LANs," *IEEE Transactions on Vehicular Technology*, vol. 62, pp. 2724–2734, jul 2013.

[35] LAN/MAN Standards Committee, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2012.

[36] D. Simon, B. Aboba, and T. Moore, "IEEE 802.11 security and 802.1 X," *IEEE document*, vol. 802, no. 1, pp. 0–1, 2000.

[37] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, MobiCom '01, (New York, NY, USA), pp. 180–189, ACM, 2001.

[38] J. Yeo, M. Youssef, and A. Agrawala, "A Framework for Wireless LAN Monitoring and Its Applications," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, WiSe '04, (New York, NY, USA), pp. 70–79, ACM, 2004.

[39] J.-C. Chen, M.-C. Jiang, and Y.-w. Liu, "Wireless LAN security and IEEE 802.11i," *IEEE Wireless Communications*, vol. 12, pp. 27–36, feb 2005.

[40] I. H. Huang, K. C. Chang, Y. C. Lu, and C. Z. Yang, "Countermeasures against MAC address spoofing in public wireless networks using lightweight agents," in *2010 The 5th Annual ICST Wireless Internet Conference (WICON)*, pp. 1–7, mar 2010.

[41] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1 X standard," tech. rep., 2002.

[42] P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese, "IEEE 802.1 X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," tech. rep., 2003.

[43] G. Escudero-Andreu, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, D. J. Parish, D. Santoro, and M. Vadursi, "A Data Fusion Technique to Detect Wireless Network Virtual Jamming Attacks," in *2015 IEEE International Workshop on Measurements & Networking (M&N)*, pp. 1–6, IEEE, oct 2015.

[44] G. T. G. Thamilarasu, S. M. S. Mishra, and R. S. R. Sridhar, "A Cross-layer Approach to Detect Jamming Attacks in Wireless Ad hoc Networks," *MILCOM 2006 - 2006 IEEE Military Communications conference*, pp. 1–7, oct 2006.

[45] A. G. Fragkiadakis, V. A. Siris, N. E. Petroulakis, and A. P. Traganitis, "Anomaly-based Intrusion Detection of Jamming Attacks, Local Versus Collaborative Detection," *Wireless Communications and Mobile Computing*, vol. 15, no. 2, pp. 276–294, 2015.

[46] M. Raya, I. Aad, J.-P. Hubaux, and A. El Fawal, "DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots," *Mobile Computing, IEEE Transactions on*, vol. 5, pp. 1691–1705, dec 2006.

[47] "Long Term Evolution (LTE) will meet the promise of global mobile broadband," *Nokia Siemens Networks*, 2009.

[48] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, (New York, NY, USA), pp. 46–57, ACM, 2005.

[49] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, WiSe '04, (New York, NY, USA), pp. 80–89, ACM, 2004.

[50] I. Bilogrevic, M. Jadliwala, and J. Hubaux, "Security Issues in Next Generation Mobile Networks: LTE and Femtocells," in *2nd International Femtocell Workshop, Luton, UK*, pp. 1–3, Citeseer, 2010.

[51] M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks," *International Journal of Information and Electronics Engineering*, vol. 2, no. 1, pp. 69–77, 2012.

[52] 3GPP TS 22.278, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet System (EPS)," *Network*, vol. 0, no. v.12.1.0 - Release 12, pp. 1–34, 2012.

[53] 3GPP TS 36.331, "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification," *Sophia*, vol. 0, no. v.10.3.0 - Release 10, 2011.

[54] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," 2013.

[55] J.-S. Cho, D. Kang, S. Kim, J. Oh, and C. Im, "Secure UMTS/EPS Authentication and Key Agreement," in *Future Information Technology, Application, and Service* (T. Park, James J. (Jong Hyuk) and Leung, Victor C.M. and Wang, Cho-Li and Shon, ed.), pp. 75–82, Springer Netherlands, 2012.

[56] 3GPP TS 36.300, "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2," no. v.14.0.2 - Release 14, 2017.

[57] D. Wetteroth, *OSI Reference Model for Telecommunications*. McGraw-Hill Professional, 2001.

[58] M. Khan, A. Ahmed, and A. R. Cheema, "Vulnerabilities of UMTS Access Domain Security Architecture," in *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08.*, pp. 350–355, IEEE, 2008.

[59] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, "Signaling oriented denial of service on LTE networks," in *Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access*, MobiWac '12, (New York, NY, USA), pp. 153–158, ACM, 2012.

[60] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–14, 2014.

[61] L. Xiehua and W. Yongjun, "Security Enhanced Authentication and Key Agreement Protocol for LTE / SAE Network," *Technology*, pp. 0–3, 2011.

[62] G. M. Køien, "Mutual Entity Authentication for LTE," *ieeexplore.ieee.org*, pp. 689–694, 2011.

[63] Y. Zheng, D. He, W. Yu, and X. Tang, "Trusted Computing-Based Security Architecture For 4G Mobile Networks," *Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, pp. 251–255, 2005.

[64] Y. Zheng, D. He, and X. Tang, "AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform," *, Communications and*, pp. 976–980, 2005.

[65] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, and D. J. Parish, "An on-line wireless attack detection system using multi-layer data fusion," in *IEEE International Workshop on Measurements and Networking Proceedings (MN)*, pp. 1–5, 2011.

[66] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, and D. J. Parish, "A multi-layer data fusion system for Wi-Fi attack detection using automatic belief assignment," in *World Congress on Internet Security (WorldCIS-2012)*, pp. 45–50, jun 2012.

[67] D. Yu and D. Frincke, "Alert confidence fusion in intrusion detection systems with extended Dempster-Shafer theory," *Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43*, vol. 2, p. 142, 2005.

[68] C. C. Tuan, Y. C. Wu, W. S. Chang, and W. T. Huang, "Fault Tolerance by Quartile Method in Wireless Sensor and Actor Networks," in *2010 International Conference on Complex, Intelligent and Software Intensive Systems*, pp. 758–763, feb 2010.

[69] K. G. Kyriakopoulos, F. J. Aparicio-Navarro, and D. J. Parish, "Manual and Automatic Assigned Thresholds in Multi-layer Data Fusion Intrusion Detection System for 802.11 Attacks," *IET Information Security*, vol. 8, no. 1, pp. 42–50, 2014.

[70] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, D. J. Parish, and J. A. Chambers, "Adding contextual information to Intrusion Detection Systems using Fuzzy Cognitive Maps," in *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 180–186, mar 2016.

[71] C. Siaterlis and B. Maglaris, "Towards Multisensor Data Fusion for DoS Detection," in *Proceedings of the 2004 ACM Symposium on Applied Computing*, SAC '04, (New York, NY, USA), pp. 439–446, ACM, 2004.

[72] UK Legislation, "Wireless Telegraphy Act 2006," 2006.

[73] R. Flöter and V. S. Systems, "PCI/CardBus 802.11a WirelessLAN driver for Atheros AR5k chipsets," 2004.

[74] V. Jacobson, C. Leres, and S. McCanne, "Libpcap, Lawrence Berkeley Laboratory, Berkeley, CA," *Initial public release June*, 1994.

[75] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, and K. Gibbs, "Iperf: The TCP/UDP bandwidth measurement tool," *htt p://dast. nlanr. net/Projects*, 2005.

[76] G. Piro, L. A. Grieco, G. Boggia, F. Capozzi, and P. Camarda, "Simulating LTE Cellular Systems: An Open-Source Framework," *IEEE Transactions on Vehicular Technology*, vol. 60, pp. 498–513, feb 2011.

[77] G. Piro, N. Baldo, and M. Miozzo, "An LTE Module for the Ns-3 Network Simulator," in *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, SIMUTools '11, (ICST, Brussels, Belgium, Belgium), pp. 415–422, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.

[78] J. Postel, "RFC 793: Transmission Control Protocol," 1981.

[79] J. Postel, "RFC 768: User Datagram Protocol," tech. rep., 1980.

[80] K. C. Leung and V. O. K. Li, "Transmission control protocol (TCP) in wireless networks: issues, approaches, and challenges," *IEEE Communications Surveys Tutorials*, vol. 8, no. 4, pp. 64–79, 2006.

[81] F. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part II - The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE Transactions on Communications*, vol. 23, pp. 1417–1433, dec 1975.

[82] D. L. Olson and D. Delen, *Advanced data mining techniques*. Springer Science {&} Business Media, 2008.

[83] M. E. Elhamahmy, H. N. Elmahdy, and I. A. Saroit, "A New Approach for Evaluating Intrusion Detection System," *Artificial Intelligent Systems and Machine Learning*, vol. 2, no. 11, pp. 290–298, 2010.

[84] O. Galinina, A. Pyattaev, S. Andreev, M. Dohler, and Y. Koucheryavy, "5G Multi-RAT LTE-WiFi Ultra-Dense Small Cells: Performance Dynamics, Architecture, and Trends," *IEEE Journal on Selected Areas in Communications*, vol. 33, pp. 1224–1240, jun 2015.

[85] G. Escudero-Andreu, R. C. Phan, and D. J. Parish, "Analysis and Design of Security for Next Generation 4G Cellular Networks," in *The 13th Annual Post Graduate Symposium on the Convergence of Telecomunications, Networking and Broadcasting, PGNET* (M. Merabti and O. Abuelmaatti, eds.), (Liverpool, UK), pp. 56–61, The School of Computing and Mathematical Sciences, Liverpool John Moores University, 2012.

[86] D. Santoro, G. Escudero-Andreu, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, D. J. Parish, and M. Vadursi, "A hybrid intrusion detection system for virtual jamming attacks on wireless networks," *Measurement*, vol. 109, pp. 79–87, may 2017.

[87] A. AlEroud and G. Karabatis, *Using Contextual Information to Identify Cyber-Attacks*, pp. 1–16. Cham: Springer International Publishing, 2017.

[88] A. Sadighian, S. T. Zargar, J. M. Fernandez, and A. Lemay, "Semantic-based context-aware alert fusion for distributed Intrusion Detection Systems," in *2013 International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pp. 1–6, oct 2013.

[89] Y. Meng and L.-F. Kwok, "Adaptive non-critical alarm reduction using hash-based contextual signatures in intrusion detection," *Computer Communications*, vol. 38, pp. 50–59, feb 2014.

APPENDIX A

Supplementary Results

Legend for IEEE 802.11

Case	Metrics Used	Case	Metrics Used
1	$\Delta Time$	17	$\Delta Time, CRC$
2	T	18	T, CRC
3	$\Delta Time, T$	19	Time, T, CRC
4	DiffFSN	20	DiffFSN, CRC
5	$\Delta Time, DiffFSN$	21	$\Delta Time, DiffFSN, CRC$
6	T,DiffFSN	22	T, DiffFSN, CRC
7	$\Delta Time, T, DiffFSN$	23	$\Delta Time, T, DiffFSN, CRC$
8	NAV	24	NAV, CRC
9	$\Delta Time, NAV$	25	$\Delta Time, NAV, CRC$
10	T, NAV	26	T, NAV, CRC
11	$\Delta Time, T, NAV$	27	$\Delta Time, T, NAV, CRC$
12	DiffFSN, NAV	28	DiffFSN, NAV, CRC
13	$\Delta Time, DiffFSN, NAV$	29	$\Delta Time, DiffFSN, NAV, CRC$
14	T, DiffFSN, NAV	30	T, DiffFSN, NAV, CRC
15	$\Delta Time, T, DiffFSN, NAV$	31	$\Delta Time, T, DiffFSN, NAV, CRC$
16	CRC		

Table A.1 Legend for IEEE 802.11 Test Case

All the results displayed on this appendix have been normalised to follow the same case nomenclature while reducing the space required to display the set of metrics selected on each iteration. The data was generated using an automated loop process which iterates through all the existing combinations of metrics selection and sliding window size. Applying the

detection algorithm on each case, it is possible to reveal the optimal combination/s to enhance the detection rate and minimise the false positive/negative alarms.

Table A.1 shows the combination of metrics selected on each experiment case ID, and the size of the SW used to compute the partial BPA values. All the scenarios follow a cycle of 31 metric combination for each sliding window size, which is the equivalent to the binary permutations of the 5 available metrics $(2^5 - 1)$, subtracting the null permutation equal to 2^0, when no metric is selected.

Additional Results for IEEE 802.11

Table A.2 IEEE 802.11 - Full List of Results for Test 1

Scenario	Case	TN	TP	FN	FP	DR	OSR
1	1	20638	29887	6290	86999	82.613%	35.132%
	2	82830	14405	21772	24807	39.818%	67.612%
	3	82788	14413	21764	24849	39.840%	67.588%
	4	67807	428	35749	39830	1.183%	47.447%
	5	73298	378	35799	34339	1.045%	51.230%
	6	92744	184	35993	14893	0.509%	64.617%
	7	82925	334	35843	24712	0.923%	57.894%
	8	107470	36177	0	163	100.000%	99.887%
	9	20638	29887	6290	86999	82.613%	35.132%
	10	82830	14413	21764	24807	39.840%	67.617%
	11	82785	25159	11018	24852	69.544%	75.058%
	12	67807	428	35749	39830	1.183%	47.447%
	13	73298	378	35799	34339	1.045%	51.230%
	14	92741	334	35843	14896	0.923%	64.719%
	15	82925	334	35843	24712	0.923%	57.894%
	16	104420	0	36177	3222	0.000%	72.605%
	17	107640	0	36177	0	0.000%	74.845%
	18	107640	0	36177	0	0.000%	74.845%
	19	107640	0	36177	0	0.000%	74.845%
	20	107640	0	36177	0	0.000%	74.845%
	21	107640	0	36177	0	0.000%	74.845%
	22	107640	0	36177	0	0.000%	74.845%
	23	107640	0	36177	0	0.000%	74.845%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	24	107640	0	36177	0	0.000%	74.845%
	25	107640	0	36177	0	0.000%	74.845%
	26	107640	0	36177	0	0.000%	74.845%
	27	107640	0	36177	0	0.000%	74.845%
	28	107640	0	36177	0	0.000%	74.845%
	29	107640	0	36177	0	0.000%	74.845%
	30	107640	0	36177	0	0.000%	74.845%
	31	107500	24	36153	140	0.066%	74.764%
2	1	21320	19499	287	71789	98.549%	36.157%
	2	80008	6	19780	13101	0.030%	70.875%
	3	70665	81	19705	22444	0.409%	62.665%
	4	85691	450	19336	7418	2.274%	76.302%
	5	74469	538	19248	18640	2.719%	66.440%
	6	91020	6	19780	2089	0.030%	80.629%
	7	88983	195	19591	4126	0.986%	78.992%
	8	84155	19786	0	8954	100.000%	92.069%
	9	21320	19499	287	71789	98.549%	36.157%
	10	77671	81	19705	15438	0.409%	68.871%
	11	70665	81	19705	22444	0.409%	62.665%
	12	85383	547	19239	7726	2.765%	76.115%
	13	73876	2936	16850	19233	14.839%	68.038%
	14	90912	202	19584	2197	1.021%	80.707%
	15	88791	312	19474	4318	1.577%	78.926%
	16	76146	0	19786	16963	0.000%	67.449%
	17	93109	0	19786	0	0.000%	82.474%
	18	93109	0	19786	0	0.000%	82.474%
	19	93109	0	19786	0	0.000%	82.474%
	20	93109	0	19786	0	0.000%	82.474%
	21	93109	0	19786	0	0.000%	82.474%
	22	93109	0	19786	0	0.000%	82.474%
	23	92716	0	19786	393	0.000%	82.126%
	24	93109	0	19786	0	0.000%	82.474%
	25	93109	0	19786	0	0.000%	82.474%
	26	93109	0	19786	0	0.000%	82.474%
	27	93109	0	19786	0	0.000%	82.474%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	28	93109	0	19786	0	0.000%	82.474%
	29	93109	0	19786	0	0.000%	82.474%
	30	93052	0	19786	57	0.000%	82.423%
	31	92709	0	19786	400	0.000%	82.120%
3	1	30559	27217	5674	80108	82.749%	40.246%
	2	108010	1187	31704	2662	3.609%	76.062%
	3	108010	1187	31704	2662	3.609%	76.062%
	4	72334	207	32684	38333	0.629%	50.531%
	5	78295	177	32714	32372	0.538%	54.662%
	6	108980	12	32879	1692	0.036%	75.919%
	7	92284	132	32759	18383	0.401%	64.375%
	8	110520	32891	0	147	100.000%	99.898%
	9	30559	27217	5674	80108	82.749%	40.246%
	10	108010	1187	31704	2662	3.609%	76.062%
	11	107990	17444	15447	2674	53.036%	87.377%
	12	72334	207	32684	38333	0.629%	50.531%
	13	78295	177	32714	32372	0.538%	54.662%
	14	108960	132	32759	1704	0.401%	75.993%
	15	92284	132	32759	18383	0.401%	64.375%
	16	11824	32891	0	98843	100.000%	31.148%
	17	30559	27217	5674	80108	82.749%	40.246%
	18	108010	1187	31704	2662	3.609%	76.062%
	19	72701	17444	15447	37966	53.036%	62.793%
	20	72334	207	32684	38333	0.629%	50.531%
	21	78295	177	32714	32372	0.538%	54.662%
	22	92284	132	32759	18383	0.401%	64.375%
	23	92284	132	32759	18383	0.401%	64.375%
	24	11824	32891	0	98843	100.000%	31.148%
	25	30559	27217	5674	80108	82.749%	40.246%
	26	107990	17444	15447	2674	53.036%	87.377%
	27	72701	17444	15447	37966	53.036%	62.793%
	28	72334	207	32684	38333	0.629%	50.531%
	29	78295	177	32714	32372	0.538%	54.662%
	30	92284	132	32759	18383	0.401%	64.375%
	31	92282	180	32711	18385	0.547%	64.407%

Scenario	Case	TN	TP	FN	FP	DR	OSR
4	1	34071	5220	1375	90026	79.151%	30.064%
	2	123940	0	6595	158	0.000%	94.833%
	3	123820	0	6595	278	0.000%	94.741%
	4	98493	1956	4639	25604	29.659%	76.859%
	5	100570	1540	5055	23529	23.351%	78.129%
	6	117370	22	6573	6732	0.334%	89.820%
	7	115580	80	6515	8517	1.213%	88.498%
	8	120200	6595	0	3895	100.000%	97.020%
	9	34071	5220	1375	90026	79.151%	30.064%
	10	123900	0	6595	198	0.000%	94.802%
	11	120210	256	6339	3887	3.882%	92.175%
	12	98493	1956	4639	25604	29.659%	76.859%
	13	100570	1540	5055	23529	23.351%	78.129%
	14	117000	80	6515	7097	1.213%	89.585%
	15	115580	209	6386	8517	3.169%	88.597%
	16	101230	0	6595	22863	0.000%	77.459%
	17	124100	0	6595	0	0.000%	94.954%
	18	124100	0	6595	0	0.000%	94.954%
	19	124100	0	6595	0	0.000%	94.954%
	20	124100	0	6595	0	0.000%	94.954%
	21	124100	0	6595	0	0.000%	94.954%
	22	124100	0	6595	0	0.000%	94.954%
	23	124010	0	6595	85	0.000%	94.889%
	24	124100	0	6595	0	0.000%	94.954%
	25	124100	0	6595	0	0.000%	94.954%
	26	124100	0	6595	0	0.000%	94.954%
	27	124100	0	6595	0	0.000%	94.954%
	28	124100	0	6595	0	0.000%	94.954%
	29	124100	0	6595	0	0.000%	94.954%
	30	124070	0	6595	23	0.000%	94.936%
	31	124010	0	6595	89	0.000%	94.886%
5	1	25980	14077	3339	96226	80.828%	28.690%
	2	81422	600	16816	40784	3.445%	58.746%
	3	81422	600	16816	40784	3.445%	58.746%
	4	94026	2902	14514	28180	16.663%	69.422%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	5	95991	2371	15045	26215	13.614%	70.449%
	6	112450	257	17159	9752	1.476%	80.725%
	7	104550	840	16576	17659	4.823%	75.481%
	8	118540	17416	0	3662	100.000%	97.377%
	9	25980	14077	3339	96226	80.828%	28.690%
	10	81422	600	16816	40784	3.445%	58.746%
	11	81403	5054	12362	40803	29.019%	61.922%
	12	94026	2902	14514	28180	16.663%	69.422%
	13	95991	2371	15045	26215	13.614%	70.449%
	14	112440	840	16576	9770	4.823%	81.131%
	15	104550	1087	16329	17659	6.241%	75.658%
	16	15728	17416	0	106480	100.000%	23.738%
	17	25980	14077	3339	96226	80.828%	28.690%
	18	81422	600	16816	40784	3.445%	58.746%
	19	68368	5054	12362	53838	29.019%	52.586%
	20	94026	2902	14514	28180	16.663%	69.422%
	21	95991	2371	15045	26215	13.614%	70.449%
	22	104550	840	16576	17659	4.823%	75.481%
	23	101120	1087	16329	21083	6.241%	73.204%
	24	15728	17416	0	106480	100.000%	23.738%
	25	25980	14077	3339	96226	80.828%	28.690%
	26	81403	5054	12362	40803	29.019%	61.922%
	27	68368	5054	12362	53838	29.019%	52.586%
	28	94026	2902	14514	28180	16.663%	69.422%
	29	95991	2371	15045	26215	13.614%	70.449%
	30	104550	1087	16329	17659	6.241%	75.658%
	31	98772	2058	15358	23434	11.817%	72.216%
6	1	45968	4062	1306	89474	75.671%	35.530%
	2	84065	149	5219	51377	2.776%	59.807%
	3	72008	2509	2859	63434	46.740%	52.920%
	4	111540	1959	3409	23900	36.494%	80.606%
	5	113530	1927	3441	21915	35.898%	81.993%
	6	122330	1044	4324	13111	19.449%	87.618%
	7	119700	1154	4214	15743	21.498%	85.827%
	8	132370	5368	0	3069	100.000%	97.820%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	9	45918	5282	86	89524	98.398%	36.361%
	10	83952	2595	2773	51490	48.342%	61.464%
	11	71599	3059	2309	63843	56.986%	53.020%
	12	111540	1959	3409	23900	36.494%	80.606%
	13	113530	1927	3441	21915	35.898%	81.993%
	14	122320	1154	4214	13118	21.498%	87.691%
	15	119700	1154	4214	15743	21.498%	85.827%
	16	23211	5368	0	112230	100.000%	20.296%
	17	34305	5282	86	101140	98.398%	28.113%
	18	60914	2595	2773	74528	48.342%	45.103%
	19	44908	3059	2309	90534	56.986%	34.065%
	20	111540	1959	3409	23900	36.494%	80.606%
	21	113530	1927	3441	21915	35.898%	81.993%
	22	119700	1154	4214	15743	21.498%	85.827%
	23	119690	1154	4214	15756	21.498%	85.818%
	24	23211	5368	0	112230	100.000%	20.296%
	25	34305	5282	86	101140	98.398%	28.113%
	26	60843	3059	2309	74599	56.986%	45.382%
	27	44908	3059	2309	90534	56.986%	34.065%
	28	111540	1959	3409	23900	36.494%	80.606%
	29	113530	1927	3441	21915	35.898%	81.993%
	30	119690	1607	3761	15748	29.937%	86.145%
	31	117580	1637	3731	17858	30.496%	84.668%
7	1	15346	26323	4328	69062	85.880%	36.215%
	2	43273	20552	10099	41135	67.052%	55.472%
	3	43273	20552	10099	41135	67.052%	55.472%
	4	72916	584	30067	11492	1.905%	63.880%
	5	75322	489	30162	9086	1.595%	65.889%
	6	79734	387	30264	4674	1.263%	69.635%
	7	78948	388	30263	5460	1.266%	68.952%
	8	82414	30651	0	1994	100.000%	98.267%
	9	15346	26323	4328	69062	85.880%	36.215%
	10	43273	20552	10099	41135	67.052%	55.472%
	11	43273	20552	10099	41135	67.052%	55.472%
	12	72916	584	30067	11492	1.905%	63.880%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	13	75322	489	30162	9086	1.595%	65.889%
	14	79719	388	30263	4689	1.266%	69.623%
	15	78938	390	30261	5470	1.272%	68.945%
	16	81689	0	30651	2719	0.000%	70.997%
	17	84408	0	30651	0	0.000%	73.361%
	18	84408	0	30651	0	0.000%	73.361%
	19	84408	0	30651	0	0.000%	73.361%
	20	84408	0	30651	0	0.000%	73.361%
	21	84408	0	30651	0	0.000%	73.361%
	22	84408	0	30651	0	0.000%	73.361%
	23	81082	136	30515	3326	0.444%	70.588%
	24	84408	0	30651	0	0.000%	73.361%
	25	84408	0	30651	0	0.000%	73.361%
	26	84408	0	30651	0	0.000%	73.361%
	27	84408	0	30651	0	0.000%	73.361%
	28	84408	0	30651	0	0.000%	73.361%
	29	84408	0	30651	0	0.000%	73.361%
	30	84359	136	30515	49	0.444%	73.436%
	31	80962	387	30264	3446	1.263%	70.702%
8	1	44608	17372	8951	72551	65.996%	43.197%
	2	80758	5500	20823	36401	20.894%	60.118%
	3	80748	5500	20823	36411	20.894%	60.111%
	4	108960	89	26234	8198	0.338%	76.002%
	5	98575	104	26219	18584	0.395%	68.774%
	6	107700	80	26243	9461	0.304%	75.116%
	7	107370	172	26151	9789	0.653%	74.952%
	8	86193	26323	0	30966	100.000%	78.418%
	9	39956	22034	4289	77203	83.706%	43.204%
	10	76489	9789	16534	40670	37.188%	60.132%
	11	74516	8977	17346	42643	34.103%	58.191%
	12	106520	120	26203	10640	0.456%	74.322%
	13	97775	430	25893	19384	1.634%	68.444%
	14	107210	193	26130	9954	0.733%	74.852%
	15	106750	181	26142	10412	0.688%	74.524%
	16	17635	26323	0	99524	100.000%	30.637%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	17	30684	22034	4289	86475	83.706%	36.742%
	18	67699	9789	16534	49460	37.188%	54.005%
	19	60822	8977	17346	56337	34.103%	48.647%
	20	94958	120	26203	22201	0.456%	66.265%
	21	95202	430	25893	21957	1.634%	66.651%
	22	105530	193	26130	11633	0.733%	73.682%
	23	104060	181	26142	13095	0.688%	72.653%
	24	17635	26323	0	99524	100.000%	30.637%
	25	30684	22034	4289	86475	83.706%	36.742%
	26	61467	13266	13057	55692	50.397%	52.085%
	27	60821	8977	17346	56338	34.103%	48.646%
	28	94385	615	25708	22774	2.336%	66.210%
	29	95129	523	25800	22030	1.987%	66.665%
	30	104940	274	26049	12220	1.041%	73.329%
	31	101710	1241	25082	15445	4.715%	71.754%
9	1	27432	10844	1069	91547	91.027%	29.242%
	2	75700	3341	8572	43279	28.045%	60.386%
	3	75672	3345	8568	43307	28.079%	60.368%
	4	113080	153	11760	5895	1.284%	86.511%
	5	113390	138	11775	5593	1.158%	86.731%
	6	113860	187	11726	5117	1.570%	87.132%
	7	108540	611	11302	10440	5.129%	83.389%
	8	73555	11913	0	45424	100.000%	65.297%
	9	79506	10844	1069	39473	91.027%	69.026%
	10	103420	3345	8568	15560	28.079%	81.567%
	11	97172	5236	6677	21807	43.952%	78.239%
	12	116790	153	11760	2191	1.284%	89.342%
	13	111320	1851	10062	7660	15.538%	86.461%
	14	114820	611	11302	4160	5.129%	88.187%
	15	114820	611	11302	4160	5.129%	88.187%
	16	12317	11913	0	106660	100.000%	18.512%
	17	27432	10844	1069	91547	91.027%	29.242%
	18	75672	3345	8568	43307	28.079%	60.368%
	19	65604	5236	6677	53375	43.952%	54.121%
	20	113080	153	11760	5895	1.284%	86.511%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	21	102160	1851	10062	16822	15.538%	79.461%
	22	108540	611	11302	10440	5.129%	83.389%
	23	108540	611	11302	10440	5.129%	83.389%
	24	73555	11913	0	45424	100.000%	65.297%
	25	79506	10844	1069	39473	91.027%	69.026%
	26	97172	5236	6677	21807	43.952%	78.239%
	27	97172	5236	6677	21807	43.952%	78.239%
	28	110410	2012	9901	8566	16.889%	85.891%
	29	111320	1851	10062	7660	15.538%	86.461%
	30	114820	611	11302	4160	5.129%	88.187%
	31	111700	1591	10322	7277	13.355%	86.554%
10	1	26949	11242	3418	69258	76.685%	34.448%
	2	51211	5259	9401	44996	35.873%	50.935%
	3	51183	5263	9397	45024	35.900%	50.913%
	4	85271	1421	13239	10936	9.693%	78.195%
	5	86196	1219	13441	10011	8.315%	78.847%
	6	88313	593	14067	7894	4.045%	80.192%
	7	88985	913	13747	7222	6.228%	81.086%
	8	81912	14660	0	14295	100.000%	87.106%
	9	25118	12345	2315	71089	84.209%	33.791%
	10	51208	5263	9397	44999	35.900%	50.936%
	11	50197	8196	6464	46010	55.907%	52.669%
	12	85271	1421	13239	10936	9.693%	78.195%
	13	86196	1219	13441	10011	8.315%	78.847%
	14	88256	1115	13545	7951	7.606%	80.611%
	15	88872	976	13684	7335	6.658%	81.041%
	16	6410	14660	0	89797	100.000%	19.005%
	17	15566	12345	2315	80641	84.209%	25.175%
	18	51183	5263	9397	45024	35.900%	50.913%
	19	46151	8196	6464	50056	55.907%	49.020%
	20	85271	1421	13239	10936	9.693%	78.195%
	21	86196	1219	13441	10011	8.315%	78.847%
	22	88060	1115	13545	8147	7.606%	80.434%
	23	87857	976	13684	8350	6.658%	80.126%
	24	6410	14660	0	89797	100.000%	19.005%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	25	15566	12345	2315	80641	84.209%	25.175%
	26	48733	10511	4149	47474	71.698%	53.437%
	27	46151	8196	6464	50056	55.907%	49.020%
	28	85271	1421	13239	10936	9.693%	78.195%
	29	86196	1219	13441	10011	8.315%	78.847%
	30	87947	1178	13482	8260	8.036%	80.389%
	31	87679	1617	13043	8528	11.030%	80.543%
11	1	4559	25005	0	174700	100.000%	14.473%
	2	168390	9	24996	10871	0.036%	82.441%
	3	145280	28	24977	33976	0.112%	71.138%
	4	167480	83	24922	11774	0.332%	82.035%
	5	158200	87	24918	21058	0.348%	77.492%
	6	178500	9	24996	759	0.036%	87.391%
	7	177910	42	24963	1344	0.168%	87.121%
	8	170010	25005	0	9249	100.000%	95.472%
	9	4559	25005	0	174700	100.000%	14.473%
	10	164450	28	24977	14807	0.112%	80.523%
	11	145280	28	24977	33976	0.112%	71.138%
	12	167460	87	24918	11801	0.348%	82.024%
	13	157620	145	24860	21634	0.580%	77.238%
	14	178400	42	24963	854	0.168%	87.361%
	15	177780	47	24958	1480	0.188%	87.057%
	16	174720	0	25005	4539	0.000%	85.536%
	17	4559	25005	0	174700	100.000%	14.473%
	18	168390	9	24996	10871	0.036%	82.441%
	19	145280	28	24977	33976	0.112%	71.138%
	20	167480	83	24922	11774	0.332%	82.035%
	21	158200	87	24918	21058	0.348%	77.492%
	22	178500	9	24996	759	0.036%	87.391%
	23	177910	42	24963	1344	0.168%	87.121%
	24	170010	25005	0	9249	100.000%	95.472%
	25	4559	25005	0	174700	100.000%	14.473%
	26	164450	28	24977	14807	0.112%	80.523%
	27	145280	28	24977	33976	0.112%	71.138%
	28	167460	87	24918	11801	0.348%	82.024%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	29	157620	145	24860	21634	0.580%	77.238%
	30	178400	42	24963	854	0.168%	87.361%
	31	177780	47	24958	1480	0.188%	87.057%
12	1	8815	18176	0	118500	100.000%	18.552%
	2	103050	10	18166	24272	0.055%	70.833%
	3	99539	44	18132	27779	0.242%	68.445%
	4	124760	204	17972	2559	1.122%	85.889%
	5	122060	267	17909	5262	1.469%	84.075%
	6	126000	4	18172	1323	0.022%	86.601%
	7	125650	12	18164	1669	0.066%	86.369%
	8	119000	18176	0	8315	100.000%	94.285%
	9	8815	18176	0	118500	100.000%	18.552%
	10	102530	44	18132	24786	0.242%	70.501%
	11	98124	570	17606	29194	3.136%	67.834%
	12	124760	267	17909	2561	1.469%	85.931%
	13	122050	300	17876	5267	1.651%	84.093%
	14	125920	12	18164	1400	0.066%	86.554%
	15	125460	136	18040	1859	0.748%	86.323%
	16	7656	18176	0	119660	100.000%	17.755%
	17	8815	18176	0	118500	100.000%	18.552%
	18	99539	44	18132	27779	0.242%	68.445%
	19	89345	570	17606	37973	3.136%	61.800%
	20	122020	267	17909	5296	1.469%	84.051%
	21	118750	300	17876	8567	1.651%	81.825%
	22	125650	12	18164	1669	0.066%	86.369%
	23	124700	136	18040	2622	0.748%	85.799%
	24	7656	18176	0	119660	100.000%	17.755%
	25	8815	18176	0	118500	100.000%	18.552%
	26	98124	570	17606	29194	3.136%	67.834%
	27	88628	12445	5731	38690	68.469%	69.469%
	28	122020	300	17876	5301	1.651%	84.070%
	29	118670	339	17837	8651	1.865%	81.795%
	30	125460	136	18040	1859	0.748%	86.323%
	31	123320	160	18016	4000	0.880%	84.868%

Legend for LTE

Following the same example, the LTE results displayed on this appendix have been normalised to follow the same case nomenclature while reducing the space required to show the set of metrics selected on each iteration, as indicated in Table A.3.

Case	Metrics Used
1	CRR
2	SMT
3	CRR, SMT
4	SR
5	CRR, SR
6	SMT, SR
7	CRR, SMT, SR height

Table A.3 Legend for IEEE 802.11 Test Case

Additional Results for LTE

The following Table A.4 contain the list of TP, TN, FP and FN obtained on each LTE scenario, as well as the two main detection performance indicators already discussed in the previous chapters: the DR and OSR.

Table A.4 IEEE 802.11 - Full List of Results for Test 1

Scenario	Case	TN	TP	FN	FP	DR	OSR
1	1	74	206	4	37	98.095%	87.227%
	2	34	204	6	77	97.143%	74.143%
	3	111	202	8	0	96.190%	97.508%
	4	74	186	24	37	88.571%	80.997%
	5	34	178	32	77	84.762%	66.044%
	6	111	176	34	0	83.810%	89.408%
	7	111	174	36	0	82.857%	88.785%
2	1	46	1096	0	0	100.000%	100.000%
	2	46	1083	13	0	98.814%	98.862%
	3	45	1069	27	1	97.536%	97.548%
	4	45	1069	27	1	97.536%	97.548%
	5	45	1069	27	1	97.536%	97.548%

Scenario	Case	TN	TP	FN	FP	DR	OSR
	6	45	1063	33	1	96.989%	97.023%
	7	46	1050	46	0	95.803%	95.972%
3	1	199	1181	1	27	99.915%	98.011%
	2	199	1181	1	27	99.915%	98.011%
	3	214	1104	78	12	93.401%	93.608%
	4	214	1104	78	12	93.401%	93.608%
	5	214	1104	78	12	93.401%	93.608%
	6	214	937	245	12	79.272%	81.747%
	7	226	5	1177	0	0.423%	16.406

APPENDIX B

MATLAB Implementation of Detection Algorithm

Main File and Configuration Parameters

The main file is used to load the matrix with all the data samples for each metric. The configuration parameters allow to tailor the detection algorithm with the desired sliding window size, aggregating the samples in groups to compute average values or specify the combination of metrics to be tested.

Once the configuration parameters are defined, this script will call to all the auxiliary functions to perform the different processes composing the detection algorithm. Finally, an output file is generated and tagged with the name specified in the configuration parameters, together with the indexed of the metrics used to perform the analysis.

```
close all
clear all
clc

% METRIC INDEXES IN INPUT FILE
% 1 > type
% 2 > subtype
% 3 > deltatime
% 4 > throughput
% 5 > diffdt
% 6 > nav
% 7 > crc
% 8 > flag
```

```
14
15 for filenum=1:1:12
16     %% LOAD SCENARIO DATA
17     clearvars -except filenum;
18     step = 5;
19     counter=1;
20     data_file = './data/test';
21     data_file = strcat(data_file, num2str(filenum));
22     data_file = strcat(data_file, '.mat');
23
24     load(data_file);
25     data = all_stats(:, 3:10);
26     flags = data(:, 8);
27     grouped = NaN;
28     % data = data(15:length(data), :);
29
30     %COMPUTE ALL THE METRIC COMBINATIONS (BINARY PERMUTATIONS)
31     permutations = zeros(31, 5);
32
33     for p=1:1:31
34         permutations(p,:) = de2bi(p,5);
35     end
36
37     permutations (:, 1) = permutations (:, 1) * 3;
38     permutations (:, 2) = permutations (:, 2) * 4;
39     permutations (:, 3) = permutations (:, 3) * 5;
40     permutations (:, 4) = permutations (:, 4) * 6;
41     permutations (:, 5) = permutations (:, 5) * 7;
42
43     % LOOP FOR INCREASING SLIDING WINDOW SIZE
44     for c=0:step:50;
45
46         sw_numsamples = c;
47         if (sw_numsamples==0)
48             sw_numsamples = 2;
49         end
```

```
50
51          for i = 1:1:31
52              % ADD ACTIVE METRICS TO metrics_index
53              metrics_index = [];
54              for j=1:length(permutations(i,:))
55                  if (permutations (i,j) > 0)
56                      metrics_index = [metrics_index permutations(i,j)];
57                  end
58              end
59
60              %% INITIALIZATION
61              % sliding window
62              buffers = zeros(length(metrics_index), sw_numsamples);
63              % algorithm notations
64              ann = zeros(length(data), 1);
65              % BPA values for each metric and sample
66              bpas = zeros(length(data), length(metrics_index), 3);
67              % Overall BPA values
68              obpas = zeros(length(data), 3);
69
70              %
71              new_data = [ ];
72
73              for k1 = 1:length(metrics_index)
74
75                  new_data = [ new_data data(:, metrics_index(k1)) ];
76
77              end
78
79              data_computed = new_data;
80
81              % GROUP METRIC SAMPLES (WHEN IT IS REQUIRED)
82              if ~isnan(grouped)
83
84                  %
85                  new_data = [ ];
```

```
86                  new_flags = [ ];
87
88                  for k1 = 1:grouped:(length(data_computed) - grouped - 1)
89
90                      rvector = [ ];
91
92                      for k2 = 1:length(metrics_index)
93
94                          t = data_computed(k1:(k1 + grouped - 1), k2);
95                          t(find(isnan(t))) = [ ];
96
97                          rvector = [ rvector mean(t) ];
98
99                      end
100
101                     new_data = [ new_data; rvector ];
102
103                     new_flags = [ new_flags; double(sum(flags(k1:(k1 +
                            grouped - 1))>0)) ];
104
105                 end
106
107                 data_computed = new_data;
108                 flags = new_flags;
109
110                 ann = zeros(length(data_computed), 1);
111                 bpas = zeros(length(data_computed), length(metrics_index)
                        , 3);
112                 obpas = zeros(length(data_computed), 3);
113
114             end
115
116             % LOAD THE BUFFERS
117             for k1 = 1:length(metrics_index)
118
119                 t = data_computed(:, k1);
```

```
120             t(find(isnan(t))) = [ ];
121             buffers(k1, :) = t(1:sw_numsamples);
122 
123         end
124 
125         %% COMPUTE BPAS
126         for k1 = sw_numsamples+1:length(data_computed)
127 
128             for k2 = 1:length(metrics_index)
129 
130                 if isnan(data_computed(k1, k2))
131 
132                     continue;
133 
134                 end
135 
136                 [ t_n_bpa t_a_bpa t_u_bpa ] = calculate_bpas(buffers(
                        k2, :), data_computed(k1, k2));
137 
138                 bpas(k1, k2, 1) = t_n_bpa;
139                 bpas(k1, k2, 2) = t_a_bpa;
140                 bpas(k1, k2, 3) = t_u_bpa;
141 
142                 new_buffer = update_buffer(buffers(k2, :), bpas(k1,
                        k2, :), data_computed(k1, k2));
143 
144                 buffers(k2, :) = new_buffer;
145 
146             end
147 
148             [ n_obpa a_obpa u_obpa ] = calculate_obpa(bpas(k1, :, :))
                    ;
149             obpas(k1, 1) = n_obpa;
150             obpas(k1, 2) = a_obpa;
151             obpas(k1, 3) = u_obpa;
152 
```

```
153                 ann(k1) = isAttack(n_obpa, a_obpa, u_obpa);
154
155             end
156
157             %% ALGORITHM PERFORMANCE ASSESSMENT
158             tp = sum(flags & ann);
159             fn = sum((flags - ann) == 1);
160             fp = sum((flags - ann) == -1);
161             tn = length(ann) -tp -fn -fp;
162
163             fnr = fn / ( tp + fn );
164             dr = tp / ( tp + fn );
165             fpr = fp / length(ann);
166
167             %% DEFINE OUTPUT FILE
168             filename = './Test';
169             filename = strcat(filename, num2str(filenum));
170             filename = strcat(filename, '/');
171             filename = strcat(filename, num2str(counter));
172             filename = strcat(filename, '_Results_SW_');
173             filename = strcat(filename, num2str(sw_numsamples));
174             filename = strcat(filename, '_Metrics_');
175
176             for k1 = 1:length(metrics_index)
177
178                 filename = strcat(filename, num2str(metrics_index(k1)));
179
180             end
181
182             save(filename);
183             a_res = [counter dr fnr fpr tn tp fn fp];
184
185             output_file = './Test';
186             output_file = strcat(output_file, num2str(filenum));
187             output_file = strcat(output_file, '/results_test');
188             output_file = strcat(output_file, num2str(filenum));
```

```
            output_file = strcat(output_file, '.csv');
            dlmwrite(output_file, a_res, '-append');
            counter = counter + 1;
        end
    end
end
```

A_BPA Function This function is responsible for computing the probability for the Attack hypothesis (without the correcting factor).

```
function bpa = calculate_a_bpa( buffer, sample )

mmax = max(buffer);

[ mmode fmax ] = mode(buffer);

dmax = mmax - mmode;

angle_max = acos( fmax / sqrt( dmax^2 + fmax^2 ) );

d = sample - mmode;

angle = acos ( fmax / sqrt( d^2 + fmax^2 ) );

if angle >= angle_max

    bpa = 0.5;

else

    bpa = 0.5*angle/angle_max;

end

end
```

BPAS Function

All the individual BPA values, which have been previously computed, are merged on this function by applying the correcting factor.

```
function [ n_bpa a_bpa u_bpa ] = calculate_bpas( buffer, sample )

 n_bpa = calculate_n_bpa(buffer, sample);
 a_bpa = calculate_a_bpa(buffer, sample);
 u_bpa = calculate_u_bpa(n_bpa, a_bpa);

 avalue = ( (n_bpa + a_bpa + u_bpa) - 1 ) / 3;

 n_bpa = n_bpa - avalue;
 a_bpa = a_bpa - avalue;
 u_bpa = u_bpa - avalue;

end
```

DS_BPA Function

This function fuses the BPA values obtained for two different observers into a final belief using D-S theory.

```
function [ obpa ] = calculate_dsbpa( bpa1, bpa2 )

obpa = [ 0 0 0 ];

beltab = zeros(3, 3);

t = bpa1(1)*bpa2(2) + bpa1(2)*bpa2(1);
t = 1 - t;

obpa(1) = bpa1(1)*bpa2(1) + bpa1(1)*bpa2(3) + bpa1(3)*bpa2(1);
obpa(2) = bpa1(2)*bpa2(2) + bpa1(2)*bpa2(3) + bpa1(3)*bpa2(2);
obpa(3) = bpa1(3)*bpa2(3);

if t == 0

    obpa(3) = 1;

```

```
else

    obpa = obpa./t;

end

end
```

N_BPA Function

This function is responsible for computing the BPA values for the Normal hypothesis (without the correcting factor).

```
function bpa = calculate_n_bpa( buffer, sample )

        mmin = min(buffer);
        mmax = max(buffer);

        q = quantile(buffer, [0.25 0.50 0.75]);
        q1 = q(1);
        me = q(2);
        q3 = q(3);

        if sample == me
                bpa = 0.5;
        else
                cond1 = q1 < sample < me;
                cond2 = me < sample < q3;

                if cond1 || cond2
                        bpa = 0.4;
                else
                        cond1 = mmin < sample < q1;
                        cond2 = q3 < sample < mmax;

                        if cond1 || cond2
                                bpa = 0.3;
                        else
                                bpa = 0.15;
```

```
                        end
                end
        end
end
```

O_BPA Function

The purpose of this function is to compute the final decision based on the individual beliefs obtained for each hypothesis.

```
function [ n_obpa a_obpa u_obpa ] = calculate_obpa( bpas )

        n_obpa = 0;
        a_obpa = 0;
        u_obpa = 0;

        [ d1 d2 d3 ] = size(bpas);
        bpas = reshape(bpas(1, :, :), [], d3);

        if d2 == 1
                n_obpa = bpas(1, 1);
                a_obpa = bpas(1, 2);
                u_obpa = bpas(1, 3);
        else
                k1 = 1;

                while true
                        bpa1 = bpas(k1, :);
                        bpa2 = bpas(k1 + 1, :);
                        obpa = calculate_dsbpa(bpa1, bpa2);

                        bpas(k1, :) = obpa;
                        bpas(k1 + 1, :) = [ ];
                        [d1 d2] = size(bpas);

                        k1 = k1 + 1;

                        if d1 == 1
                                break;
```

```
                        end

                        if d1 == 2
                                k1 = 1;
                        end
                end

                n_obpa = bpas(1, 1);
                a_obpa = bpas(1, 2);
                u_obpa = bpas(1, 3);
        end
end
```

U_BPA Function

This function is responsible for computing the BPA values for the Uncertainty hypothesis (without the correcting factor).

```
function bpa = calculate_u_bpa( n_bpa, a_bpa )

t = [ n_bpa a_bpa ];

bpa = 0.5*min(t)/max(t);

end
```

APPENDIX C

Changes on atr5k-driver for IEEE 802.11 WNIC

Due to space limits, only the two modified files are included in this appendix. The entire method affected by the changes has been quoted, to facilitate the understanding of the way the DoS attack has been implemented. The driver's source code used on this thesis is an extender version of the original Linux kernel driver for Atheros chipsets. The source code was created by R. Flöter using reverse-engineering techniques, and is distributed under a GNU General Public License as published. The copyright rights belong to its authors.

The initial comments of each file have been preserved on this quotation to emphasise that the author of this thesis has not contributed in any manner on the development of this source-code. Only two minor amendments were included on the original code, as highlighted with the green comments, to be able to implement the attacker behaviour. For further information, please consult the full implementation of the ar5k-driver for the Atheros chipsets [73].

HACK 1: Disable Contention Window

```
1 /*
2  * Copyright (c) 2004–2008 Reyk Floeter <reyk@openbsd.org>
3  * Copyright (c) 2006–2008 Nick Kossifidis <mickflemm@gmail.com>
4  * Copyright (c) 2007–2008 Pavel Roskin <proski@gnu.org>
5  *
6  * Permission to use, copy, modify, and distribute this software for any
7  * purpose with or without fee is hereby granted, provided that the above
8  * copyright notice and this permission notice appear in all copies.
9  *
```

```
10  * THE SOFTWARE IS PROVIDED 'AS IS' AND THE AUTHOR DISCLAIMS ALL
        WARRANTIES
11  * WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
12  * MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE
        FOR
13  * ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
14  * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
15  * ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
        OF
16  * OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
17  *
18  */
19
20 [...] // OTHER METHODS HAVE BEEN OMITTED
21
22 /*
23  * Initialize the 4-word tx control descriptor on 5212
24  */
25 static int ath5k_hw_setup_4word_tx_desc(struct ath5k_hw *ah,
26         struct ath5k_desc *desc, unsigned int pkt_len, unsigned int
            hdr_len,
27         int padsize,
28         enum ath5k_pkt_type type, unsigned int tx_power, unsigned int
            tx_rate0,
29         unsigned int tx_tries0, unsigned int key_index,
30         unsigned int antenna_mode, unsigned int flags,
31         unsigned int rtscts_rate,
32         unsigned int rtscts_duration)
33 {
34         struct ath5k_hw_4w_tx_ctl *tx_ctl;
35         unsigned int frame_len;
36
37         tx_ctl = &desc->ud.ds_tx5212.tx_ctl;
38
39         /*
40          * Validate input
```

```
41          * - Zero retries don't make sense.
42          * - A zero rate will put the HW into a mode where it continously
                sends
43          *   noise on the channel, so it is important to avoid this.
44          */
45         if (unlikely(tx_tries0 == 0)) {
46                 ATH5K_ERR(ah->ah_sc, zero retries);
47                 WARN_ON(1);
48                 return -EINVAL;
49         }
50         if (unlikely(tx_rate0 == 0)) {
51                 ATH5K_ERR(ah->ah_sc, zero rate);
52                 WARN_ON(1);
53                 return -EINVAL;
54         }
55
56         tx_power += ah->ah_txpower.txp_offset;
57         if (tx_power > AR5K_TUNE_MAX_TXPOWER)
58                 tx_power = AR5K_TUNE_MAX_TXPOWER;
59
60         /* Clear descriptor */
61         memset(&desc->ud.ds_tx5212, 0, sizeof(struct
               ath5k_hw_5212_tx_desc));
62
63         /* Setup control descriptor */
64
65         /* Verify and set frame length */
66
67         /* remove padding we might have added before */
68         frame_len = pkt_len - padsize + FCS_LEN;
69
70         if (frame_len & ~AR5K_4W_TX_DESC_CTL0_FRAME_LEN)
71                 return -EINVAL;
72
73         tx_ctl->tx_control_0 = frame_len & AR5K_4W_TX_DESC_CTL0_FRAME_LEN
               ;
```

```
74
75          /* Verify and set buffer length */
76
77          /* NB: beacon's BufLen must be a multiple of 4 bytes */
78          if (type == AR5K_PKT_TYPE_BEACON)
79                  pkt_len = roundup(pkt_len, 4);
80
81          if (pkt_len & ~AR5K_4W_TX_DESC_CTL1_BUF_LEN)
82                  return -EINVAL;
83
84          tx_ctl->tx_control_1 = pkt_len & AR5K_4W_TX_DESC_CTL1_BUF_LEN;
85
86          tx_ctl->tx_control_0 |=
87                  AR5K_REG_SM(tx_power, AR5K_4W_TX_DESC_CTL0_XMIT_POWER) |
88                  AR5K_REG_SM(antenna_mode,
                        AR5K_4W_TX_DESC_CTL0_ANT_MODE_XMIT);
89          tx_ctl->tx_control_1 |= AR5K_REG_SM(type,
90                                  AR5K_4W_TX_DESC_CTL1_FRAME_TYPE);
91          tx_ctl->tx_control_2 = AR5K_REG_SM(tx_tries0,
92                                  AR5K_4W_TX_DESC_CTL2_XMIT_TRIES0);
93          tx_ctl->tx_control_3 = tx_rate0 & AR5K_4W_TX_DESC_CTL3_XMIT_RATE0
                ;
94
95  #define _TX_FLAGS(_c, _flag)                                    \
96          if (flags & AR5K_TXDESC_##_flag) {                      \
97                  tx_ctl->tx_control_##_c |=                      \
98                          AR5K_4W_TX_DESC_CTL##_c##_##_flag;      \
99          }
100
101         _TX_FLAGS(0, CLRDMASK);
102         _TX_FLAGS(0, VEOL);
103         _TX_FLAGS(0, INTREQ);
104         _TX_FLAGS(0, RTSENA);
105         _TX_FLAGS(0, CTSENA);
106         _TX_FLAGS(1, NOACK);
107
```

```
108 #undef _TX_FLAGS
109
110         /*
111          * WEP crap
112          */
113         if (key_index != AR5K_TXKEYIX_INVALID) {
114                 tx_ctl->tx_control_0 |=
                        AR5K_4W_TX_DESC_CTL0_ENCRYPT_KEY_VALID;
115                 tx_ctl->tx_control_1 |= AR5K_REG_SM(key_index,
116                         AR5K_4W_TX_DESC_CTL1_ENCRYPT_KEY_IDX);
117         }
118
119         /*
120          * RTS/CTS
121          */
122         if (flags & (AR5K_TXDESC_RTSENA | AR5K_TXDESC_CTSENA)) {
123                 if ((flags & AR5K_TXDESC_RTSENA) &&
124                                 (flags & AR5K_TXDESC_CTSENA))
125                         return -EINVAL;
126                 /*************
127                 ORIGINAL VALUE
128                 **************/
129                 /*tx_ctl->tx_control_2 |= rtscts_duration &
130                                 AR5K_4W_TX_DESC_CTL2_RTS_DURATION;*/
131
132                 /*********************************************
133                 CHANGE TO SET NAV DURATION TO THE MAXIMUM VALUE
134                 *********************************************/
135                 tx_ctl->tx_control_2 |= AR5K_4W_TX_DESC_CTL2_RTS_DURATION
                        ;
136                 tx_ctl->tx_control_3 |= AR5K_REG_SM(rtscts_rate,
137                                 AR5K_4W_TX_DESC_CTL3_RTS_CTS_RATE);
138         }
139
140         return 0;
141 }
```

```
142
143 [...] // OTHER METHODS HAVE BEEN OMITTED
```

HACK 2: NAV Value Set to Maximum Value

```
1  /*-
2   * Copyright (c) 2002-2005 Sam Leffler, Errno Consulting
3   * Copyright (c) 2004-2005 Atheros Communications, Inc.
4   * Copyright (c) 2006 Devicescape Software, Inc.
5   * Copyright (c) 2007 Jiri Slaby <jirislaby@gmail.com>
6   * Copyright (c) 2007 Luis R. Rodriguez <mcgrof@winlab.rutgers.edu>
7   *
8   * All rights reserved.
9   *
10  * Redistribution and use in source and binary forms, with or without
11  * modification, are permitted provided that the following conditions
12  * are met:
13  * 1. Redistributions of source code must retain the above copyright
14  *    notice, this list of conditions and the following disclaimer,
15  *    without modification.
16  * 2. Redistributions in binary form must reproduce at minimum a
    disclaimer
17  *    similar to the 'NO WARRANTY' disclaimer below ('Disclaimer') and
    any
18  *    redistribution must be conditioned upon including a substantially
19  *    similar Disclaimer requirement for further binary redistribution.
20  * 3. Neither the names of the above-listed copyright holders nor the
    names
21  *    of any contributors may be used to endorse or promote products
    derived
22  *    from this software without specific prior written permission.
23  *
24  * Alternatively, this software may be distributed under the terms of the
25  * GNU General Public License (GPL) version 2 as published by the Free
26  * Software Foundation.
27  *
28  * NO WARRANTY
29  * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
```

```
30  * ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
31  * LIMITED TO, THE IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTIBILITY
32  * AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
33  * THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR SPECIAL, EXEMPLARY
        ,
34  * OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
        OF
35  * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
        BUSINESS
36  * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
37  * IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
        OTHERWISE)
38  * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF
39  * THE POSSIBILITY OF SUCH DAMAGES.
40  *
41  */
42
43  [...] // OTHER METHODS HAVE BEEN OMITTED
44
45  /**************\
46  * Queues setup *
47  \**************/
48
49  static struct ath5k_txq *
50  ath5k_txq_setup(struct ath5k_softc *sc,
51                  int qtype, int subtype)
52  {
53          struct ath5k_hw *ah = sc->ah;
54          struct ath5k_txq *txq;
55          struct ath5k_txq_info qi = {
56                  .tqi_subtype = subtype,
57                  /* XXX: default values not correct for B and XR channels,
58                   * but who cares? */
59                  .tqi_aifs = AR5K_TUNE_AIFS,
60                  /**************
61                  ORIGINAL VALUE
```

```
62                 **************/
63                 //.tqi_cw_min = AR5K_TUNE_CWMIN,
64                 //.tqi_cw_max = AR5K_TUNE_CWMAX
65                 /***********************************
66                 CHANGE TO ELIMINATE CONTENTION WINDOW
67                 ***********************************/
68                 .tqi_cw_min = 0,
69                 .tqi_cw_max = 0
70         };
71         int qnum;
72
73         /*
74          * Enable interrupts only for EOL and DESC conditions.
75          * We mark tx descriptors to receive a DESC interrupt
76          * when a tx queue gets deep; otherwise we wait for the
77          * EOL to reap descriptors.  Note that this is done to
78          * reduce interrupt load and this only defers reaping
79          * descriptors, never transmitting frames.  Aside from
80          * reducing interrupts this also permits more concurrency.
81          * The only potential downside is if the tx queue backs
82          * up in which case the top half of the kernel may backup
83          * due to a lack of tx descriptors.
84          */
85         qi.tqi_flags = AR5K_TXQ_FLAG_TXEOLINT_ENABLE |
86                                 AR5K_TXQ_FLAG_TXDESCINT_ENABLE;
87         qnum = ath5k_hw_setup_tx_queue(ah, qtype, &qi);
88         if (qnum < 0) {
89                 /*
90                  * NB: don't print a message, this happens
91                  * normally on parts with too few tx queues
92                  */
93                 return ERR_PTR(qnum);
94         }
95         if (qnum >= ARRAY_SIZE(sc->txqs)) {
96                 ATH5K_ERR(sc, 'hw qnum %u out of range, max %tu!\n', qnum
                    , ARRAY_SIZE(sc->txqs));
```

```
97                  ath5k_hw_release_tx_queue(ah, qnum);
98                  return ERR_PTR(-EINVAL);
99          }
100         txq = &sc->txqs[qnum];
101         if (!txq->setup) {
102                 txq->qnum = qnum;
103                 txq->link = NULL;
104                 INIT_LIST_HEAD(&txq->q);
105                 spin_lock_init(&txq->lock);
106                 txq->setup = true;
107                 txq->txq_len = 0;
108                 txq->txq_poll_mark = false;
109                 txq->txq_stuck = 0;
110         }
111         return &sc->txqs[qnum];
112 }
113
114 [...] // OTHER METHODS HAVE BEEN OMITTED
```