A Channel Selection Model based on Trust Metrics for Wireless Communications

Claudio Marche, Valeria Loscri, Michele Nitti

A Channel Selection Model based on Trust Metrics for Wireless Communications

Claudio Marche, *Graduate Student Member, IEEE,* Valeria Loscri, *Senior Member, IEEE,* and Michele Nitti, *Senior Member, IEEE*

***Abstract*—Dynamic allocation of frequency resources to nodes in a wireless communication network is a well-known method adopted to mitigate potential interference, both unintentional and malicious. Various selection approaches have been adopted in literature, to limit the impact of interference and keep a high quality of wireless links. In this paper, we propose a different channel selection method, based on trust policies. The trust management approach proposed in this work relies on the node's own experience and trust recommendations provided by its neighbourhood. By means of simulation results in Network Simulator NS-3, we demonstrate the effectiveness of the proposed trust method, while the system is under jamming attacks, in respect of a baseline approach. We also consider and evaluate the resilience of our approach in respect of malicious nodes, providing false information regarding the quality of the channel, to induct bad channel selection of the node. Results show how the system is resilient in respect of malicious nodes, keeping around 10% of throughput more than an approach only based on the own proper experience, considering the presence of 40% of malicious nodes, both single and collusive attacks.**

***Index Terms*—Countermeasure In Wireless Networks, Communications Channel Selection, Trustworthiness Management, Jamming Attacks.**

I. Introduction

The ubiquitous connotation of wireless devices, pushed by the advent of 5G and new technologies such as Artificial Intelligence (AI), is contributing to making wireless services a daily life presence.

The wireless network capacity has been drastically boosted, with the advent of new services and the constant evolution of wireless towards 802.11ax for the Wi-Fi and the 5th generation (5G) of cellular systems [1], [2]. The high-speed services based on wireless technologies are expected to become still more ubiquitous and support a massive deployment of wireless communicating objects, enabling the Internet of Everything (IoE) paradigm. The IoE concept encompasses things, processes, people and data [3]. The inherent openness of wireless technology, together with its increasing use, makes security threats increase as well. In particular, wireless communication networks are very sensitive to interference: a mitigation approach adopted to face this interference effect is channel hopping. It is a method that allocates in a dynamic way the frequencies to the nodes in a wireless communication system. Different approaches have been proposed in the literature, with the main objective of mitigating interference, both unintentional and malicious.

In this last case, we talk about Denial of Service (DoS) attacks, which can be realized as a jamming/adversarial attack against a victim receiver. The effectiveness of this kind of attack is increased exponentially with the newly developed techniques, such as reactive jamming, where the jammer decides where to focus for maximum impact by performing a cognitive radio sensing [4].

In these terms, we propose a channel selection model able to assist wireless nodes in choosing the best channel to transmit on, that is suitable for wireless devices and does not require standard modifications. The proposed model, developed for wireless technologies based on the association phase, can be implemented in several wireless technologies, spanning from IEEE 802.15.4 to Z-Wave, just to cite a few. As follows, we were inspired by the concept of trustworthiness and took advantage of the well-known trust management techniques. In this scenario, the communication between nodes involves two different roles: the first represents the trustor, and it has to trust the other one, which depicts the trustee and provides the required data. However, misbehaving devices can perform different types of attacks and can disrupt communications for their own gain. The trustworthiness management techniques have to solve the essential issue to detect which channel is affected by malicious behaviours and so lead the nodes to successful collaboration. Our paper works in this direction, intending to estimate the best wireless channel and avoid jamming interference, and thus provides the following contributions:

- First, we propose a trust management model, based on experience and recommendations, able to assist wireless nodes in channel selection, that does not require any standard modification. Thanks to the model, the nodes should select the best reliable channel so as to prevent jamming attacks or other interference.
- Second, we analyze different behaviours of jamming attacks and propose a new dynamic one, which is then used to test the resiliency of our model and the common wireless approaches.
- Third, we conduct extensive evaluations by comparing the proposed channel selection algorithm with two models, i.e. the classical approach described in the 802.11 standards and another one that considers only the past experiences of nodes. The evaluation results show the

C. Marche and M. Nitti are with the Department of Electrical and Electronic Engineering (DIEE), University of Cagliari, Italy.

C. Marche and M. Nitti are with National Telecommunication Inter University Consortium, Research Unit of Cagliari, Italy.

V. Loscri is with INRIA Lille-Nord Europe, Lille, France.

E-mails: C.M. claudio.marche@unica.it, V.L. valeria.loscri@inria.fr and M.N. michele.nitti@unica.it.

importance of the experience and recommendation to prevent jamming attacks and, moreover, the influence of the time windows in dynamic jamming ones.

The rest of the article is organized as follows: Section II presents a brief survey on channel selection, the possible types of jamming attacks and the importance of trust mechanisms in wireless networks. In Section III, we describe the scenario and introduce the used notations. Section IV illustrates the proposed trust management model, while Section V provides details of simulations and results. We conclude the paper with a brief discussion and some final remarks in Section VI.

II. Related Works

In this Section, we focus on the most representative works related to three different key aspects of our approach. The first aspect revises the most representative jamming attacks described in the literature, while the second one evaluates the channel selection mechanisms used to mitigate the interference impact, which could be effective also against jamming. Moreover, we finalize this Section by reporting the most recent works on trust algorithms adopted in wireless networks.

A. Jammer Attacks

The massive use in our daily life of wireless services makes security threats an important concern to be considered, above all in terms of availability of wireless communications, data integrity, etc [5]. The interference from other networks produced by simultaneous transmissions, i.e., inter-network interference, significantly reduces the network throughput and affects all the ongoing transmissions [6]. Radio jamming is certainly one of the major threats to which wireless networks are particularly prone. With the advancement of the software-defined radio approaches, it has become quite easy to launch a jamming attack [7]. Despite the increasing evolution of wireless communication technologies, most of them are vulnerable to jamming attacks, due to the lack of adequate countermeasures.

There are several types of jamming attacks, some of them were initially conceived for Wi-Fi technology but have been then proven to be effective also for other types of wireless networks. Among them, we can count constant jamming attacks [8], where the jammer constantly broadcasts a signal over time. Even though this type of attack is really effective, by reaching a 100% of packet error rate, its main weakness is the energetic inefficiency. Another type of well-known attack in literature is reactive jamming, relying on the knowledge of the channel from the attacker, that sends an interference based on the detection of a legitimate transmitted packet [9]. This type of attack is more energy-efficient than constant, but it requires a tight timing constraint, on the order of $4\mu s$ for OFDM, in order to make the switching between listening and transmitting. Another weakness aspect is related to the length of the detected packet. This type of attack is ineffective for short packet sizes.

Other types of attacks are random and periodic jamming attacks. The former ones are considered memoryless attacks and consist of sending signals at random times, and then the offender switches to sleep mode [10]. In the periodic version, the attacker sends signals at precise and predefined times. They are certainly more energy efficient than constant attacks, but less effective. Other types of attacks have been expressly conceived for Wi-Fi networks, and in particular for the physical and MAC layers. One of them is represented by a timing synchronization attack. Several attacks have been proposed, able to thwart the synchronization signal time, with the main aim of disrupting the start-of-packet procedure. In particular, the authors of [11] have proposed preamble spoofing attacks, by injecting the same preamble as the legitimate user, in order to make the receiver incapable of decoding the legitimate data. Generally, this type of attack is based on a very good knowledge of the network timing. Another type of jamming attack is represented by the frequency synchronization jamming attacks, where an offset of the carrier frequency may cause a deviation from the orthogonality and introduces a phase deviation, with an important degradation of the SNR and the demodulation performance. Channel estimation jamming attacks are another type of jamming based on generating malfunctioning channel estimation and channel equalization. If the accuracy of the channel estimation is impacted as shown in [12], the degradation of the network can be very high. Anyway, the results in [12] have been proved via simulation, but nulling attacks in real-world scenarios seem complicated to be realized, due to the mismatches between the attacker and the legitimate device, both in terms of timing and phase.

The proposed approach is tested against a complex jamming strategy, namely reactive, according to which an attacker disturbs only communications that have already started and so targeting packets that are already *on the air*. Two different behaviours are implemented: a static behaviour, where the jammer can attack only a specific channel, and a new proposed dynamic one, thanks to which the jammer can change the target by jumping into different channels.

B. Channel Selection Models

This subsection provides an overview regarding the background of channel selection in wireless technologies. In recent years, the community has strongly focused on the issue of interference and jamming attacks in wireless networks, and several works have been proposed. Below, we provide a brief survey of some of the most appreciated approaches in the literature without pretending to be exhaustive.

In these terms, two well-known channel selection models based on machine learning techniques are illustrated in [13] and [14]. In the first work, the authors propose an advanced deep-learning mechanism to select available wireless channels with good quality and avoid interference from external communications. The Wi-Fi channel is selected based on the signal strength and the channel quality in terms of Channel State Information (CSI); the model proposes discarding the most crowded wireless environments. In the second work, the authors illustrate a channel assignment approach using a neural network, namely Coherent Ising Machines (CIM), operating at the quantum limit. The proposed centralized controller selects the best channel by evaluating all the information periodically

sent by the Access Points (APs); the optimization function is formulated in order to maximize the throughput and minimize the interference between APs.

Other two approaches based on machine learning techniques are illustrated in [15] and [16]. In the first work, the authors propose a combined mechanism that integrates specific machine learning algorithms and Time Slotted Channel Hopping (TSCH) in order to select high-performance channels in a ZigBee scenario. In specific, the authors evaluate 9 different Multi-Armed Bandit (MAB) algorithms and illustrate how their combination can improve the packet delivery ratio. In the second work, the authors depict a channel and spreading factor assignment to minimize the grid energy cost in a green LoRa network, powered by both a renewable energy source and the conventional grid. Based on machine learning approaches, the proposed model is then tested under different scenarios.

Moreover, an approach based on advanced machine learning algorithms is proposed in [17]. The authors illustrate a protocol based on a deep learning technique that proposes to mitigate interference through the analysis of the spectrum. The channel is sensed, and then its spectrum is analyzed and classified by a deep neural network that is responsible for detecting unusual behaviours, such as jamming attacks. Another two approaches concerning machine learning are presented in [18] and [19]. The first work depicts a decentralized learning-based channel selection approach for IoT systems. The approach allows IoT devices to select appropriate channels based on Acknowledge (ACK) information among devices, with low computational complexity. While the second work illustrates an approach for performing the channel allocation based on graph analysis and regression techniques to minimize the overlap among APs. The interference is reduced through the combination of passive measurements on the medium, such as the Received Signal Strength Indicator (RSSI), and the analysis of the behaviour of the neighbours and the community.

Moreover, channel selection models based on different techniques are depicted in the literature; among them, two works developed for a Bluetooth scenario are presented in [20] and [21]. The first work illustrates an adaptive frequency hopping technique based on linear programming, to prevent interference while keeping the communication process going. The authors propose an interference scheme based on the packet status of a BLE connection and an algorithm that helps to choose a channel based on probability. In the second work, the authors investigate various interference levels and depict an improved channel selection algorithm combining different channel maps gathered from the environment; the model is then tested analysing the relationship between transmission failure probability and packet loss rate. Another recent approach is presented in [22]. The work illustrates a model that supports assigning the best channel and selecting the spreading factor to achieve the rate demand of end devices in LoraWAN-based networks. The algorithm, simulated using Matlab, proposes to improve throughput, reduce power consumption and guarantee link reliability.

The last group of articles mainly focuses on the analysis of collaboration between devices. Among them, in [23], the authors propose a selection and allocation channel method for wireless networks for two typical scenarios, i.e. enterprise and residential. A bonding matrix is created to represent the channel usage for a considered Access Point (AP) and its neighbours. Then, a specific bandwidth is allocated for the transmission and the channel with the lowest utilization is selected. Another approach where the collaboration is analyzed is presented in [24]. The authors map the process of interference minimization into a competitive game of Game Theory, where the APs represent the players and the channels depict the possible strategies. The competition of the wireless network, i.e. the game, is tested with two different behaviours of nodes, where the first demand lower collaboration, while the other one assumes the collaboration between all the nodes in order to reach a maximum global benefit.

However, to the best of our knowledge, even though such advanced techniques depict acceptable results, these exhibit several gaps. For example, many of the presented works are not suitable for devices that are usually based on restricted and low computation capabilities, and so, often, they require the use of central entities or controllers, where complex algorithms are implemented. Furthermore, the standard modifications represent another problem: several models propose the optimization of physical or MAC frames format, which are actually already well examined and accepted by the community. Moreover, two other gaps are exhibited; the first one regards that many of these works need an additional radio unit, which should be configured in a monitor mode and can be used as support for the master unit used to give network access to the nodes, while the other lack considers that many works do not test their approaches with interference and attacks, and so authors can not estimate the resiliency in adverse scenarios. To sum it up, in Table I, we summarize the more representative contributions described above.

The approach proposed in this work aims to select the channels based on their reliability obtained considering a node's experience and the recommendations from its neighbours. The needed information to compute the channel's trust is integrated into the standard, so the approach does not need additional messages to be exchanged. Moreover, no central controllers are required, and each device can independently estimate the trustworthiness of the channel and its neighbours without an additional radio unit.

C. Trust Mechanisms in Wireless Networks

Most of the contributions on trust approaches applied in wireless networks are integrated into the routing mechanisms. Very few papers focus on spectrum allocation or channel selection based on the trust concept. One of the first contributions in this direction is [25], where the authors propose a trust algorithm that combines the trust value and the method of spectrum allocation. During the spectrum allocation, the reputation value is fixed and cannot be changed. In [26], authors combine relay selection with channel conditions information to obtain a modified trust model, that will be applied along with the source, the relay and the destination. In [27], authors take advantage of the trust concept in order to improve device-to-device (D2D) communications by gathering

TABLE I
ANALYSIS OF THE EXISTING CHANNEL SELECTION MODELS.

Ref	Approach	Scenario	No Standard modification	No central controllers	No additional radio unit	Jamming Attacks
[13]	Deep Learning	Wi-Fi	✓	✓	-	-
[14]	Neural Network	Wi-Fi	-	-	✓	-
[15]	Probability Theory	ZigBee	✓	✓	✓	-
[16]	Reinforcement Learning	LoRaWAN	✓	-	✓	-
[17]	Deep Learning	Wi-Fi	✓	✓	-	✓
[18]	Reinforcement Learning	LoRaWAN	-	✓	✓	-
[19]	Regression Analysis	Wi-Fi	✓	✓	-	-
[20]	Linear Algorithm	Bluetooth	-	✓	✓	-
[21]	Channel Map	Bluetooth	-	✓	✓	-
[22]	Mathematical Optimization	LoraWAN	-	-	✓	-
[23]	Linear Algorithm	Wi-Fi	-	-	✓	-
[24]	Game Theory	Wi-Fi	✓	-	✓	-
Our solution	Trustworthiness Management	Multi Wireless Technologies	✓	✓	✓	✓

both Quality of Service (QoS) and spectrum sensing data and weighting the received information using a social algorithm. Another approach is illustrated in [28], where the authors propose a reputation-based scheme for cooperative spectrum sensing. The approach is based on the proper knowledge of the spectrum and also relies on neighbourhood information. They also consider Spectrum Sensing Data Falsification (SSDF) attacks, based on false information regarding the sensing with the main objective of deteriorating the network's performance. The method proposed in that work is close to the approach we developed in this work, but the main important difference is that we rely on a wireless network, and we do not consider a cognitive radio context, with a distinction between primary and secondary users. In general, studies have proved the validity of the trust concept in wireless networks; however, it is necessary to investigate the attack introduced with trust management, i.e. attacks on recommendations, thanks to which the reputation of good nodes is ruined when numerous malicious objects act alone or collude together to start disseminating bad recommendations intentionally [29].

III. SCENARIO

This paper proposes a trust management model able to assist wireless nodes, both static and mobile, to choose the most trustworthy channel to transmit on. The requirements for the proposed approach are based on the distribution of the nodes and the adoption of the Frequency Hopping Spread Spectrum technique. For these reasons, technologies such as IEEE 802.15.4, ad-hoc IEEE 802.11 and Z-waves can be candidates for the trust-based framework. The innovative part stands in involving all objects in the risk assessment to allow the transmitter to select the best channel to communicate on so as to avoid any possible jammer in the network.

In our modelling, the set of wireless nodes is represented by $\mathcal{N} = \{n_1, ..., n_i, ...n_I\}$ with cardinality I, where n_i is the generic node. We can then describe the subjective topology of the network by making use of the set of distances of all the nodes in the network from node n_i as $\mathcal{D}_i = \{d_{ij} : j \neq i\}$. The neighbours of the generic node n_i are represented in our model by $\mathcal{N}_i = \{n_j \in \mathcal{N} : d_{ij} < R_i\}$ that is the set of nodes that are within the transmission range R_i of node n_i.

In the evaluated scenario, we are considering a wireless spectrum as the resource to be monitored, so let $\mathcal{C} = \{c_1, ..., c_x, ...c_X\}$ be the set of X possible channels. The goal of our paper is, for each node, to obtain a complete and trustable vision of the spectrum usage thanks to the neighbours' recommendations to avoid malicious nodes that could affect the transmission, i.e. jammers. Nevertheless, the transmitter continuously monitors the transmission in terms of Packet Delivery Ration (PDR) so that if its quality is below a certain threshold due to interference from other nodes, the communication is immediately suspended. Figure 1 shows in detail the wireless network association procedure for the nodes and the contribution of the proposed trust management model.

The whole process starts whenever an application is installed on a physical node, let us suppose node n_i, needs to transmit data to another node n_j. At first, node n_i sends probe requests to discover wireless nodes within its proximity to send data to, and if a response is received, the procedure moves to the authorization phase. After the discovery and authorization phases, node n_i has to decide on which channel to transmit its data: the proposed system makes use of the neighbours of n_i, i.e. the nodes in $\mathcal{N}_i$, to identify the most reliable channel. The selection algorithm takes into consideration the sensing power and the experience of neighbours' nodes and evaluates their recommendations, represented by n_z in Figure 1. Recommendations are integrated into the beacon frames, which are continually exchanged by wireless nodes. More details about beacon frames and recommendations will be illustrated in the next Section. As soon as the best channel is selected, the association phase starts and so node n_i communicates the chosen channel to the receiver. The last phase depicts the communication, in which the nodes transfer data and the channel is continuously monitored to guarantee the

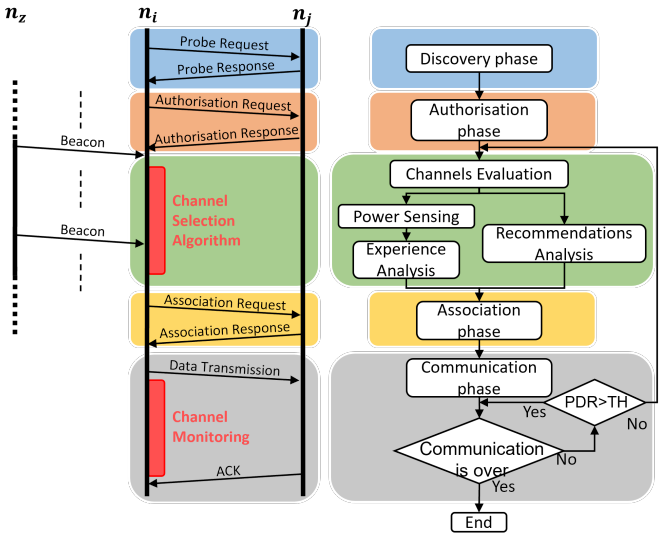


Fig. 1. Wireless association process and trust management model flowchart.

best communication in terms of PDR.

When the transmission is over, the trustworthiness values are updated. Node n_i computes the trustworthiness of its $\mathcal{N}_i$ neighbours on the basis of its own experience and of their channel recommendations; in particular, node n_i evaluates the communication over the chosen channel $e^w_{i,x}$ for transaction w so that $\mathcal{E}_{i,x}$ is the set of all the evaluation transaction of node n_i on channel c_x. Moreover, node n_i assigns a feedback f^w_{ij} to all its neighbours that provide information about the channel c_x, so that $\mathcal{F}_{ij}$ is the set of all feedback assigned from node n_i to node n_j. Both $e^w_{i,x}$ and f^w_{ij} are associated with a timestamp t_w, so that it is possible to know when they were generated and eventually discard them if they are outdated.

Finally, node n_i updates the neighbours' trustworthiness values based on the assigned feedback: we refer to this trustworthiness with T_{ij}, i.e. the trustworthiness of node n_j seen by node n_i. The details on how T_{ij} is computed are explained in Section IV.

IV. Trust Management Model

According to the presented scenario, we propose a decentralized model, where each node calculates and stores information regarding its own channel experiences and the feedback needed to calculate the trustworthiness level of its neighbours locally, so to have its own opinion about the channels' status. This is intended to avoid a single point of failure and infringement of the values of trustworthiness and to easily identify malicious attacks that change their behaviours based on the requester, such as the Discriminatory Attack. Whenever a node n_i has data to transmit, it first needs to establish a connection with the recipient node on a set channel. In order to select the most reliable transmitting channel, node n_i senses the received power P_i on each channel c_x of interest, namely $P_{i,x}$, and also consider its neighbours' evaluations regarding their past experience, integrated into the probe requests, on all the channel in order to evaluate the risk $R_{i,x}$ associated to the transmission on each channel.

TABLE II
Experiences of node n_z

		Channel				
		1	...	x	...	X
Transactions	$w=1$	$e^1_{z,1}$		$e^1_{z,x}$		$e^1_{z,X}$
	...					
	w	$e^w_{z,1}$		$e^w_{z,x}$		$e^w_{z,X}$
	...					
	$w=\lvert\mathcal{E}^*_{z,x}\rvert$	$e^{\lvert\mathcal{E}^*_{z,x}\rvert}_{z,1}$		$e^{\lvert\mathcal{E}^*_{z,x}\rvert}_{z,x}$		$e^{\lvert\mathcal{E}^*_{z,x}\rvert}_{z,X}$

Node n_i is then able to weight the received data and compute the resulting power for channel c_x as follows:

$$P_x = P_{i,x} + R_{i,x} \tag{1}$$

where the computed risk is used as an adjustment to the perceived power, to take into account the possibility of jammer nodes operating in that channel. Node n_i will consider the channel as free for transmission if the combined received power is lower than a threshold. The risk assessment is computed taking into account both node n_i's experience and the experience of its neighbours:

$$R_{i,x} = U_{i,x} + U_{\mathcal{N}_i,x} \tag{2}$$

where $U_{i,x}$ expresses the average experience of node n_i while $U_{\mathcal{N}_i,x}$ accounts for the experiences of all its neighbours, when using channel c_x over a limited time window. This is useful to take into account that channel conditions can vary over time, so we can discard any outdated evaluations. Let $\mathcal{E}^*_{z,x} = \left\{\forall e^w_{z,x} \in \mathcal{E}_{z,x} : (t_{act} - t_w) < TH\right\}$ be all the evaluations received within the last TH seconds in channel c_x for the generic node n_z. We can express its average experience as follows:

$$U_{z,x} = \sum_{w=1}^{|\mathcal{E}^*_{z,x}|} e^w_{z,x} \Big/ |\mathcal{E}^*_{z,x}| \tag{3}$$

where w indexes from the latest transaction ($w=1$) to the oldest one ($w = |\mathcal{E}^*_{z,x}|$) within the considered time limit as shown in Table II. Obviously, the number of transactions in each channel is hardly the same, so the resulting table will not be a matrix.

Node n_i will then receive and store the experiences $U_{z,x}$ from all its neighbours related to the different channel in $\mathcal{C}$, as shown in Table III and has to aggregate them in order to derive the risk associated to each channel. To this, node n_i will weight the received recommendations based on the trust level of its neighbours, as follows:

$$U_{\mathcal{N}_i,x} = \sum_{k=1}^{|\mathcal{N}_i|} T_{ik} U_{k,x} \Big/ \sum_{k=1}^{|\mathcal{N}_i|} T_{ik} \tag{4}$$

The experiences $U_{k,x}$ can be integrated into the body of beacon frames that are transmitted periodically by the wireless standard, for example in the optional fields depicted in the IEEE 802.11 [30]. In specific, the number of octets needed to

TABLE III
AVERAGE EXPERIENCE OF NODE n_i'S NEIGHBOURS

		Neighbours				
		n_1	...	n_k	...	$n_{\lvert\mathcal{N}_i\rvert}$
Channels	c_1	$U_{1,1}$		$U_{k,1}$		$U_{\lvert\mathcal{N}_i\rvert,1}$
	...					
	c_x	$U_{1,x}$		$U_{k,x}$		$U_{\lvert\mathcal{N}_i\rvert,x}$
	...					
	c_X	$U_{1,X}$		$U_{k,X}$		$U_{\lvert\mathcal{N}_i\rvert,X}$

send the recommendation for the channels strictly depends on their accuracy.

Finally, node n_i will select the channel with the minimum resulting power P_x to communicate its data. During the transmission, node n_i verifies the quality of transmission by computing the relative PDR. If the transmission is degraded, i.e. the computed PDR is below 60%, node n_i immediately suspends the transmission. In this case, node n_i checks for other available channels and, if any, changes the transmission channel so that the communication between the two nodes can continue in the new channel.

When the transmission is over, node n_i evaluates the used channel based on the PDR value. Evaluation is represented by $e^w_{i,x}$, which refers to each transaction w and it is expressed in a continuous range ($e^w_{i,x} \in [0,1]$): n_i rates 1 if it is fully satisfied by the transaction, i.e. if the PDR is 100%, and 0 otherwise, i.e. if it has to switch channel due to PDR less than 60%. However, in a realistic scenario, the PDR is hardly 100%, so in order to evaluate the communication, it is possible to implement a listening phase so that the transmitting node can obtain a reference PDR of the environment and then it can re-scale the feedback taking into account the reference PDR as the maximum value.

Intermediate values of the evaluation $e^w_{i,x}$ are computed considering the line through these two points, i.e. maximum and minimum allowed PDR, as follows:

$$e_{i,x} = 2.5PDR - 1.5 \tag{5}$$

After the evaluation of the channel, n_i computes the feedback f^w_{iz} to be assigned to the neighbours that have contributed to the computation of the resulting power P_x by providing their average experience on the channel $U_{z,x}$, so as to reward/penalize them for their advice. According to Equation 6, if a node gave a positive experience of the channel, it receives the same evaluation as the channel, namely a positive feedback if the communication was satisfactory, $e_{i,x} \geq 0.5$, and a negative one otherwise, $e_{i,x} < 0.5$; instead, if the generic neighbour n_z gave a negative evaluation, then it receives negative feedback if the communication was satisfactory and a positive one otherwise. Note that the feedback generated by node n_i are stored locally and used for future trust evaluations.

$$f^w_{iz} = \begin{cases} e_{i,x} & \text{if } U_{z,x} \geq 0.5 \\ 1 - e_{i,x} & \text{if } U_{z,x} < 0.5 \end{cases} \tag{6}$$

According to the proposed model, let $\mathcal{F}^*_{iz} = \{\forall f^w_{iz} \in \mathcal{F}_{iz} : (t_{act} - t_w) < TH\}$ be all the feedback assigned within the last TH seconds. For the generic node n_z, the transmitting node can compute the trust value of another node as follows:

$$T_{iz} = \sum_{w=1}^{|\mathcal{F}^*_{iz}|} f^w_{iz} \Big/ |\mathcal{F}^*_{iz}| \tag{7}$$

where w indexes from the latest transaction ($w = 1$) to the oldest one ($w = |\mathcal{F}^*_{iz}|$) within the considered time limit.

TABLE IV
NS-3 SETUP PARAMETERS

Parameter	Value
Area of simulation	(40x40)m
Number of packets	50
Packet dimension	1.5 kB
Protocol	IEEE 802.11g
Frequency	2.4 GHz
Number of channels	13
Bandwidth	22 MHz
Number of communications	56 per node

V. EXPERIMENTAL EVALUATION

In this Section, we will test the proposed trust algorithm in a network with one or more jammers and show how it is able to prevent disturbance and help nodes select the best wireless channel.

A. Simulation Setup

A simulation setup using the NS-3 network simulator has been developed to generate a peer-to-peer network of objects in a (40x40)m area. Each node randomly communicates with others, and each interaction consists of 50 packets with a dimension of 1.5 KB each, for a total of 75 KB of data. Information is exchanged according to the Wi-Fi 802.11g protocol in the 2.4 GHz microwave band, which makes use of 13 channels with a bandwidth equal to 22 MHz. We are considering an ad hoc scenario, where only peer-to-peer communications are allowed, i.e. there is no presence of an Access Point. The physical layer implements the AARF Rate control algorithm [31] in order to provide multi-rate capabilities, so each device is able to adapt its transmission rate dynamically. To test the validity of our approach, we analyze 1568 communications that correspond to 56 communications per node; all the following results consider a process with this value of total communications. Table IV summarizes the used configuration for the parameters in the NS-3 simulator.

Each node can play the role of either a requester or a provider, and the information travels from the provider to the requester in the selected channel. In these terms, the communication involves two different nodes: the node that sends the information, i.e. the provider, and the other one that uses the data, i.e. the requester. If the quality of the transmission drops, e.g. due to a jammer attack or a high interference, a new channel is selected according to the implemented algorithm,

and the interaction starts from the last received packet. In order to test the performance of the algorithm, we make use of different jammers. All the jammers implement a reactive strategy, targeting only packets that are already *on the air* and disturbing only communications that have already started. Therefore, two different behaviours are implemented: in the first one, called static behaviour, a jammer can attack only a specific channel, while in the second one, namely dynamic behaviour, the jammer can change the attacked channel by jumping into different channels. In this work, we focus on a random selection of the channels to be attacked.

As described in Section IV, each node is able to evaluate the trust level of its neighbours based on the received recommendations. Two main types of recommendation nodes are implemented in the network: one is always benevolent, so a node n_z provides only good recommendations, based on its experience $e_{z,x}$, while the other one is malicious, according to which a node tries to disrupt the network by sending false recommendations, i.e. $(1 - e_{z,x})$. The trust value of each recommendation node is calculated in an interval of [0,1], where if trust reaches 0, the neighbour is classified as malicious; otherwise, it is considered as benevolent, with trust equal to 1. The neighbours' reputation, i.e. their trust value, is used to weigh their recommendations, and it is useful to help the channel selection algorithm in the trust model.

We evaluate the performance by analyzing three metrics: a) the packet delivery ratio (PDR), b) the number of channel failures and c) the percentage throughput (THR). The PDR is expressed as the ratio of the total number of packets delivered to the total number of packets sent from the source node to the destination, and it is used to check the quality of each interaction. The number of channel failures refers to the number of times the device is forced to change the Wi-Fi channel due to a jammer attack or high interference. Finally, the THR represents how information can be delivered in a given amount of time and is usually presented as bit-per-second. We want to clarify that, in our simulations, the THR is influenced only by the time necessary for the communication between the two nodes, and the amount of information does not affect the score because every dropped packet is re-transmitted. Therefore, all the required data reach a destination at the end of each simulation, notwithstanding the Wi-Fi channel selection method used. In each experiment, we express the THR in terms of percentage regarding its highest value.

B. Trust Model Functioning

This section illustrates the functioning of the proposed channel selection algorithm and shows how communications can be disrupted by jamming attacks. We introduced it to show the rationale of our work. As follows, the scenario is developed with a limited number of 8 nodes that communicate with each other in a Wi-Fi area, which is busy with other external communications. Only 3 free channels are available for devices, and the channels can be affected by one or more reactive static jammers or by noise or high interference (e.g. different communications, such as Bluetooth). Each node produces data with a rate of 17 Kpbs and does not consider experiences older than $TH = 700s$. Table V summarizes the specific scenario parameters used as motivation and explanation of the functioning of the system.

TABLE V
TRUST MODEL FUNCTIONING SCENARIO PARAMETERS

Parameter	Value
Number of nodes	8
Free channels	3
Data rate	17 Kbps
Number of jammers	[1, 2, 3]
Jammer hop frequency	Static
Temporal limit to compute experience and recommendations	700 s

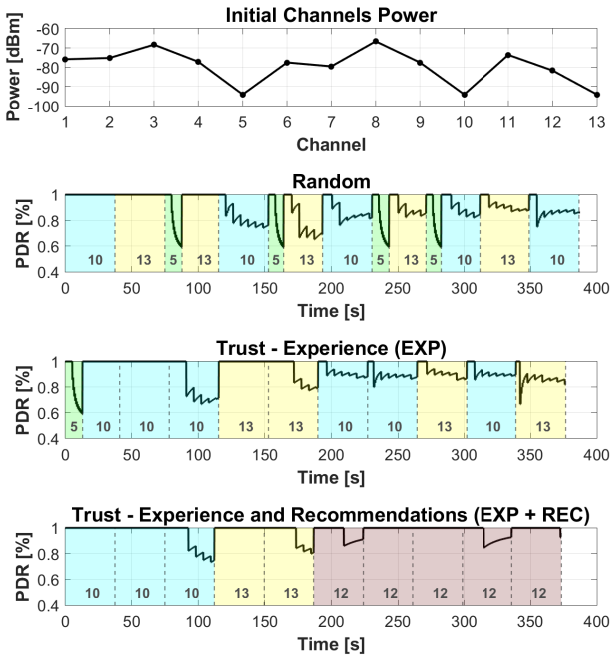


Fig. 2. Initial channel power and PDR analysis for a communication adopting the three analysed algorithms.

The proposed trust model is compared with two other approaches, i.e. a random approach, where the channel to communicate on is selected randomly and an approach where the channel selection is based only on the direct experiences of each node. Figure 2 shows a comparison from the perspective of a single node. The first graph illustrates the initial channel powers measured by the node: only channels 5, 10 and 13 are available and free, i.e. they have a power below -93 dBm, at time 0 s. Moreover, a reactive static jammer is employed in this simulation, which affects channel 5, while channels 10 and 13 are affected by other no Wi-Fi communications starting from 90 s and 170 s, respectively. All the approaches are able to discard the channels with low performance, i.e. with a PDR lower than 0.6, and select another channel. Each approach selects a new Wi-Fi channel: the random model picks a free random channel, while the other two approaches are based

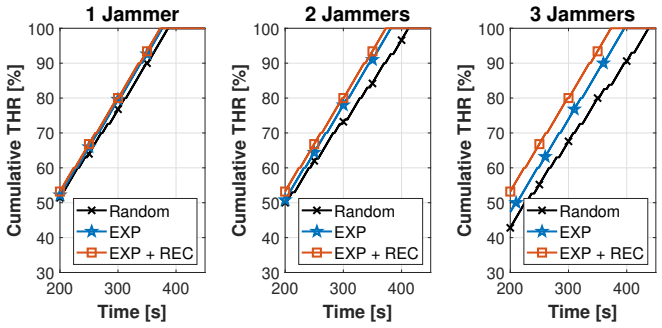


Fig. 3. Cumulative THR increasing the number of jammers for the three approaches.

on the node's direct experience and on the combination of experience and recommendations from neighbours. The graphs illustrate how the random approach is the worst in terms of performance due to the random selection of channel 5 affected by the jammer. The trust approach, based only on experience, can learn about past interactions and selects channel 5 only once. The last graph shows how the trust model, based on direct experience and recommendation, discards channel 5 from the beginning and selects a new channel rather than 10 and 13. Thanks to recommendations from neighbours, the node takes advantage of other nodes' past experiences and it is able to select another channel, i.e. channel 12, which offers it better performance even if it is involved in another Wi-Fi communication.

The next set of simulations examines the models' behaviours by increasing the number of jammers. Figure 3 illustrates the cumulative THR for different experiments with 1, 2 and 3 reactive static jammers that attack channels 5, 10 and 13, respectively. The graphs exhibit how the random approach significantly degrades its performance with the increasing number of jammers; this is due to the frequent selection of the channels affected by jammers. The two trust approaches that consider the experience and the combination of experience and recommendations show the best performance. In the first one, each node chooses the attacked channels only once, and thanks to the mechanism of experience, other channels are selected for the next interactions. Concerning the trust approach that considers recommendations, a node that selects an attacked channel informs its neighbours so that the same information is shared among all the nodes and this approach is able to reach 100% of transferred data in less time w.r.t. the other two approaches.

C. Model Performance

In this Section, we evaluate the performance of the proposed trust approach in a complete scenario. We make use of a network of 28 nodes that communicate with each other in a free WiFi area without external communications; all 13 channels can be used, and each node evaluates the best channel based on the employed approach. The performances are analyzed with different data rates and several numbers of jammers. Moreover, different jammer strategies are adopted, i.e. static and dynamic

TABLE VI
MODEL PERFORMANCE SCENARIO PARAMETERS

Parameter	Value
Number of nodes	28
Free channels	13
Data rate	[17, 24, 40, 120] kbps
Number of jammers	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]
Jammer hop frequency	Static/Dynamic
Temporal limit to compute experience and recommendations	[300, 700] s / No limit
% of malicious nodes	[0, 20, 40, 60, 80, 100] %

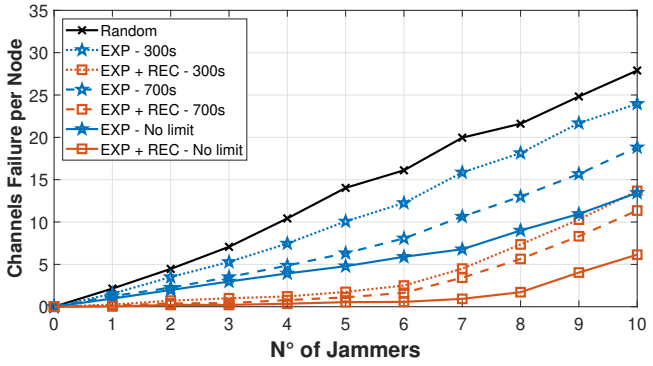


Fig. 4. Channels failure per node increasing the number of static jammers for the three approaches with different values of temporal limit.

ones and various temporal limits to computing experience and recommendations are examined. Finally, in the last set of simulations, several percentages of malicious recommendation nodes are considered in order to evaluate the impact of attacks on recommendations for the proposed trust approach. Table VI summarizes the configuration of the simulation parameters in the general scenario and the different values that can be assigned to each one.

The focus of the first set of simulations is to test how the three different approaches perform while increasing the number of jammers. Each jammer presents a reactive static behaviour, so it can attack a specific channel only if there are packets in the air. We analyze the behaviours for different values of the temporal limit to compute experience and recommendations. Figure 4 illustrates how the random approach depicts the worst behaviour due to the high number of times that selects the channel affected by a jammer. On the other hand, thanks to the analysis of past experience, the Trust - Experience approach performs better; moreover, the higher the temporal limit, the higher the performance against a static jammer that does not change the attacked channel. These types of attacks are better managed by the Trust - Experience and Recommendations approach, in which each node communicates the attacked channel to neighbours through recommendations; this dissemination of information allows the fast detection of the compromise channels, and so the selection of the best channels.

The next set of simulations examines the impact of the data rate for the three analyzed approaches. To this, we make use

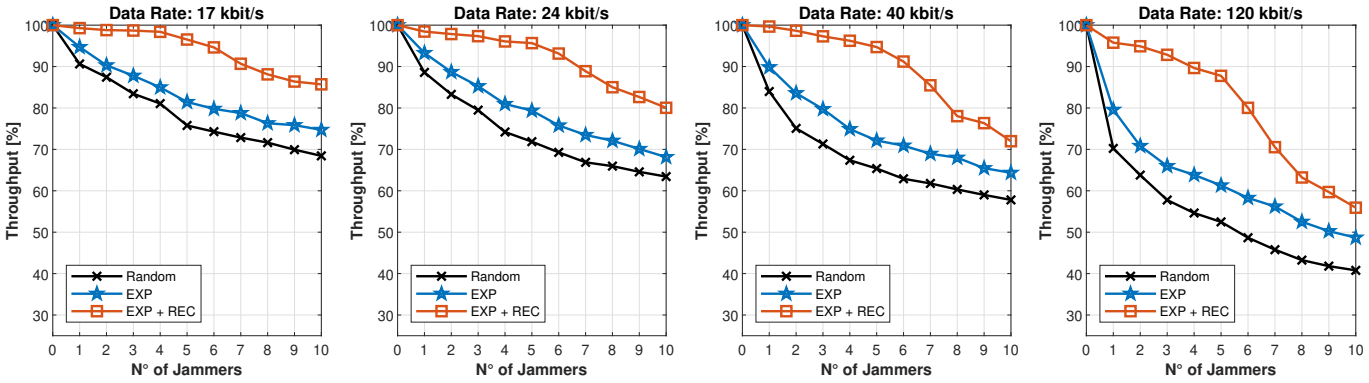


Fig. 5. Impact of Data Rate ad the variation of the number of static jammers for the three approaches.

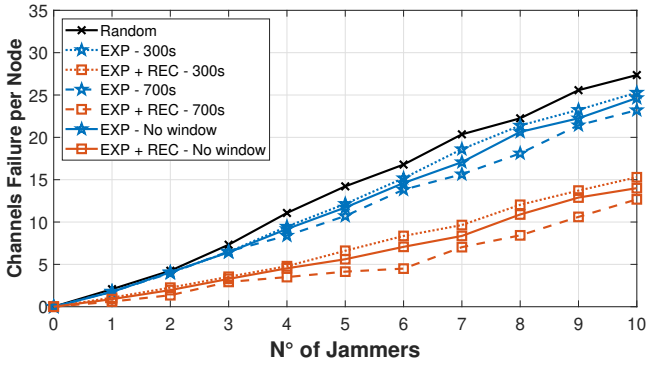


Fig. 6. Channels failure per node increasing the number of dynamic jammers with a hop frequency equal to 600s and considering different values of temporal limit for the trust approaches.

of a temporal limit of 700s for the two approaches based on trust, which does not strictly impact this experimentation. Figure 5 illustrates how with the increase of the data rate, the throughput has a different impact for all the approaches. We consider the throughput in percentage, where each subplot corresponds to the specific scenario of data rate. In general, the data rate has a direct impact on the throughput, and, in the absence of jammers, the greater the data rate, the greater the throughput, thanks to the shorter time required to send information. On the other hand, every time a jammer damages a communication, the two affected nodes, i.e. the requester and the provider, have to change the channel and proceed to a new association phase accordingly. These phases directly impact the throughput, and the time needed for communication increases. However, the approaches based on experience and recommendations overcome the classic random approach and, with up to 5 affected channels, the proposed approach is able to keep the throughput over 80%.

The focus of the next set of simulations is to test how the proposed model works with the dynamic behaviour of the jammers. We suppose that every 600s, a jammer changes its target to another channel, randomly selected. Figure 6 illustrates how the average of channel failures per node increases with the number of dynamic jammers for the three approaches and for different values of the temporal limit. The results exhibit how the trust approach, based on experience and recommendations, overcomes such attacks and shows how the approach is able to adapt to the changes in the jammer's behaviour quickly. The best performance is represented with a value of temporal limit equal to 700s, which is closest to the hop frequency of jammers and is the fastest one to recognize the dynamic behaviour rather than the other two values.

We now want to analyze the results varying the temporal limit needed to evaluate the experience and the recommendations for the two trust approaches. In order to analyze the relationship between the jammer hop frequency and the temporal limit, we make use of a higher data rate, i.e. 40 Kbit/s, since the throughput is more influenced by the temporal window. Figure 7 illustrates the percentage of throughput for different values of jammer hop frequency at increasing values of temporal limit. The graphs show how the temporal limit directly impacts only the trust approaches, while the random approach keeps a constant behaviour. As already demonstrated by the previous simulations, the best performance in terms of throughput is depicted for values of the temporal limit, which are close to the frequency hop of the jammers, while a temporal limit equal to 0 corresponds to a random approach, in which the nodes can not take advantages of the past information. Low values of temporal limit exhibit the worst performance due to the node that has to reset its memory and select the channels starting from the beginning every time. On the other side, values of limits much greater than the frequency hop can degrade the throughput in the same way. For this reason, a preliminary study of the attackers could improve the performance of the trust approaches, which, however, show the best results compared to the classical Wi-Fi approach.

Finally, the last set of simulations is aimed at understanding how the proposed approach reacts when neighbours nodes implement the two primary attacks on the recommendations. In the first one, namely *single attack*, a malicious node provides false recommendations to decrease the chance of good channels being selected for Wi-Fi communications. This is the simplest attack on recommendations, in which each node acts maliciously without considering the behaviour of its neighbours and provides false recommendations regardless

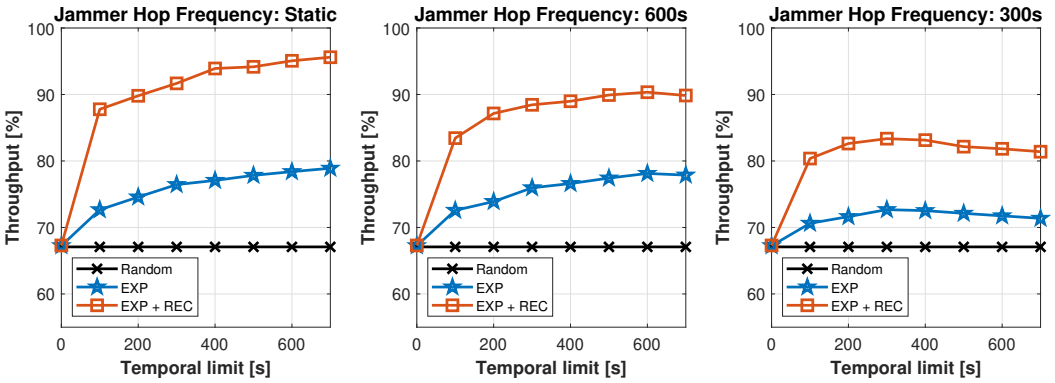


Fig. 7. Percentage of Throughput at the variation of temporal limit, for different values of jammer hop frequency.

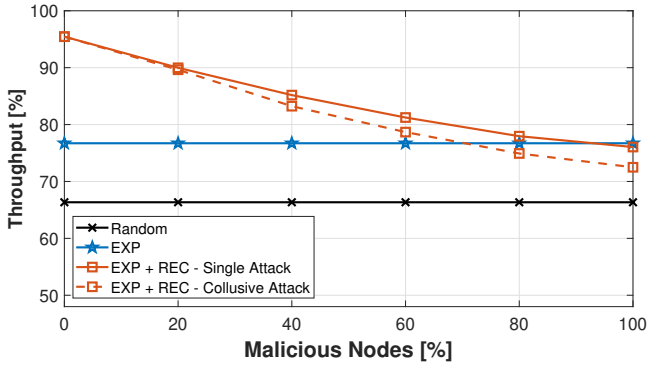


Fig. 8. Throughput percentage at increasing values of % of malicious nodes.

of the destination node. The second attack, namely *collusive attack*, represents the worst behaviour. In this attack, a group of nodes works together to increase the reputation of a bad channel, i.e. attacked by jammers, and so increase its chances of being selected as the communication channel; this represents the worst attack on recommendations in which malicious nodes collaborate together to maintain their reputation. Figure 8 illustrates the impact of such attacks on recommendations for the three different approaches in a scenario with 4 static jammers. The graph depicts how the attacks affect only the trust approach based on the recommendations, while the other two approaches have a constant behaviour. We can see how the percentage of throughput decreases with increasing the percentage of malicious nodes and reaches the lowest value with respect to the approach based on experience, even if better than the classical random approach. This is due to the necessary time to detect the attacks; when a node detects attacks on recommendations, it discards the malicious nodes after 1 or 2 interactions or even more for the collusive attack. This needed time has a direct impact on the performance and so provokes a reduction of throughput. So, for a high percentage of collusive attackers greater than 70%, the mechanism of recommendation falls and substantially reduces the percentage of throughput. However, even if the percentage of malicious nodes is high, the proposed approach performs well in comparison to the classic random approach. Finally, we want to point out that security mechanisms could prevent nodes from becoming malicious, i.e. jammers or bad recommenders, but if this happens, the information sent by the node is false but legit as it is the response to a query from the requester and can not be discarded. For this reason, trustworthiness management models are required to identify such nodes and should work together with security mechanisms to protect the network.

VI. Conclusions

In this article, we have proposed a channel selection method for wireless communications based on trust policies. The illustrated approach, developed for objects with low computational capabilities, operates as a support for several wireless standards and does not require any additional device radio unit. In specific, the proposed model is developed for wireless technologies based on the distribution of nodes, in which an important role is represented by the association phase and the main requirements are based on the adoption of a channel hopping mechanism. Applicable to a generic wireless network, each node is able to select the most trustworthy channel to transmit on, thanks to the neighbours' recommendations and its own experience.

The proposed approach has been tested against different types of security threats, in specific concerning interference from other networks or by simultaneous transmissions, and moreover against the major attacks to which wireless networks are particularly prone, i.e. the jamming attack. All the jammers implement a complex reactive strategy, disturbing only communications that have already started, and two different behaviours are considered: a static behaviour, in which a jammer can attack only a specific channel, and a dynamic one, where the jammer can change the attacked channel by jumping into different channels.

Furthermore, we have compared our solution with two other approaches, i.e. the classical approach described in the 802.11 standards and another one that considers only the past experiences of nodes. Experiments evaluation has shown that our approach is able to outperform the other two approaches when considering a network with different types of interference and jamming attacks. Future further extensions that are worth studying include the modification of the approach in order to

be implemented in an AP scenario, in which all the wireless devices communicate with each other through an access point.

REFERENCES

[1] Y. Miao *et al.*, "Fair and dynamic data sharing framework in cloud-assisted internet of everything," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7201–7212, 2019.

[2] S. Amuru *et al.*, "On jamming against wireless networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 412–428, 2017.

[3] D. J. Langley *et al.*, "The internet of everything: Smart things and their impact on business models," *Journal of Business Research*, vol. 122, pp. 853–863, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S014829631930801X

[4] S.-Y. Chang *et al.*, "Fast ip hopping randomization to secure hop-by-hop access in sdn," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 308–320, 2018.

[5] M. Yang *et al.*, "Mac technology of ieee 802.11 ax: Progress and tutorial," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1122–1136, 2021.

[6] J. Liu *et al.*, "Throughput analysis of ieee 802.11 wlans with inter-network interference," *Applied Sciences*, vol. 10, no. 6, p. 2192, 2020.

[7] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2022.

[8] K. Pelechrinis *et al.*, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[9] Y. Cai *et al.*, "Joint reactive jammer detection and localization in an enterprise wifi network," *Computer Networks*, vol. 57, no. 18, pp. 3799–3811, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128613003095

[10] E. Bayraktaroglu *et al.*, "On the performance of ieee 802.11 under jamming," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 1265–1273.

[11] M. J. L. Pan *et al.*, "Jamming attacks against ofdm timing synchronization and signal acquisition," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, 2012, pp. 1–7.

[12] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, 2011.

[13] F. Wang *et al.*, "Channel selective activity recognition with wifi: A deep learning approach exploring wideband information," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 181–192, 2018.

[14] K. Kurasawa *et al.*, "A high-speed channel assignment algorithm for dense ieee 802.11 systems via coherent ising machine," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1682–1686, 2021.

[15] H. Dakdouk *et al.*, "Reinforcement learning techniques for optimized channel hopping in ieee 802.15. 4-tsch networks," in *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2018, pp. 99–107.

[16] R. Hamdi *et al.*, "Lora-rl: Deep reinforcement learning for resource management in hybrid energy lora wireless networks," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6458–6476, 2021.

[17] K. Davaslioglu *et al.*, "Deepwifi: Cognitive wifi with deep learning," *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 429–444, 2019.

[18] A. Li *et al.*, "A lightweight decentralized reinforcement learning based channel selection approach for high-density lorawan," in *2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2021, pp. 9–14.

[19] O. Jeunen *et al.*, "A machine learning approach for ieee 802.11 channel allocation," in *2018 14th International Conference on Network and Service Management (CNSM)*. IEEE, 2018, pp. 28–36.

[20] B. Pang *et al.*, "Bluetooth low energy interference awareness scheme and improved channel selection algorithm for connection robustness," *Sensors*, vol. 21, no. 7, p. 2257, 2021.

[21] ——, "A probability-based channel selection algorithm for bluetooth low energy: A preliminary analysis," in *2021 XXX International Scientific Conference Electronics (ET)*. IEEE, 2021, pp. 1–4.

[22] S. Shraideh *et al.*, "Joint channel and spreading factor selection algorithm for lorawan based networks," in *2020 International Conference on UK-China Emerging Technologies (UCET)*. IEEE, 2020, pp. 1–4.

[23] A. Zakrzewska and L. Ho, "Dynamic channel bandwidth use through efficient channel assignment in ieee 802.11 ac networks," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–6.

[24] S. L. Gramacho *et al.*, "A game theoretical approach to model the channel selection dynamics in non-coordinated ieee 802.11 networks," *Wireless Networks*, vol. 25, no. 8, pp. 4663–4682, 2019.

[25] Q.-Q. Pei *et al.*, "A trust value-based spectrum allocation algorithm in cwsns," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 261264, 2013. [Online]. Available: https://doi.org/10.1155/2013/261264

[26] R. Changiz *et al.*, "Trust management in wireless mobile networks with cooperative communications," in *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, 2010, pp. 498–503.

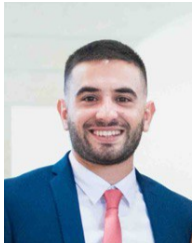
[27] M. Nitti *et al.*, "Using an iot platform for trustworthy d2d communications in a real indoor environment," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 234–245, 2018.

[28] Z. Sun *et al.*, "Reputation-based spectrum sensing strategy selection in cognitive radio ad hoc networks," *Sensors (Basel, Switzerland)*, vol. 18, 2018.

[29] W. Z. Khan *et al.*, "Trust management in social internet of things: Architectures, recent advancements, and future challenges," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7768–7788, 2020.

[30] "IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp. 1–4379, 2021.

[31] M. Lacage *et al.*, "Ieee 802.11 rate adaptation: a practical approach," in *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, 2004, pp. 126–134.



Claudio Marche Claudio Marche received his PhD in Electronic and Computer Engineering in 2023 and the M.Sc. degree in Telecommunication Engineering with full marks in 2018 at the University of Cagliari. Since graduation, he has been working as a Researcher in the Department of Electrical and Electronic Engineering at the University of Cagliari in the Net4U research group. He is currently a Researcher, and his current research interests include the Internet of Things (IoT) and Machine Learning.

Valeria Loscri is a permanent researcher at Inria Lille since Oct. 2013. She received her MSc and PhD degrees in Computer Science in 2003 and 2007, respectively, from the University of Calabria and her HDR (Habilitation à diriger des recherches) in 2018 from Université de Lille (France). Her research interests focus on cybersecurity, unconventional wireless communication paradigms as VLC, cooperation and coexistence of wireless heterogeneous devices. She has been nominated to the 2021 Women Stars in Computer Networking and Communications Communications in 2021 by the IEEE Communication Society. Since 2019, she is Scientific International Delegate for Inria Lille–Nord Europe.

Michele Nitti is an Assistant Professor at the University of Cagliari, Italy since 2015. He served as a technical program chair for various international conferences (IEEE BMSB 2017, IEEE IoT V&T Summit 2020) and workshops. Currently, he is a member of the editorial board for the IEEE IoT Journal, Elsevier Computer Networks and MDPI IoT and co-founder of an academic spin-off (GreenShare s.r.l.) which works in the mobility sector. His main research interests are in architecture and services for the Internet of Things (IoT).