Computer Communications 174 (2021) 109–121

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Countering radiometric signature exploitation using adversarial machine learning based protocol switching

Wassila Lalouani [a], Mohamed Younis [a,*], Uthman Baroudi [b]

[a] Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD, USA
[b] Computer Engineering Department, King Fahd University of Petroleum & Minerals, Dhahran, 31261, Saudi Arabia

ARTICLE INFO

Keywords:
Radiometric signature
RF fingerprinting
Traffic analysis
Distributed beamforming
Adversarial machine learning

ABSTRACT

A Radiometric signature refers to transceiver specific features that are caused by variations in the manufacturing process even for the same circuit design. While such a radiometric signature constitutes a fingerprint that can be exploited for device authentication, it is a threat to privacy. Particularly, in the realm of wireless networks, an adversary may exploit radio frequency (RF) fingerprinting to identify devices and conduct traffic analysis in order to uncover the topology and categorize the role of various nodes. In this paper, we show how an adversary could employ RF fingerprinting to distinguish among nodes and bypass the provisioned anonymity protection in the network. We analyze the accuracy of RF fingerprinting and highlight how the accuracy affects the success of adversary attacks. To counter such a threat, we propose a novel methodology that requires no hardware changes to the radio transceiver and the associated host device. Our methodology is based on coordinated switching among preset link-layer and physical-layer communication protocols. For the latter, we particularly exploit distributed beamforming. We employ adversarial machine learning to select the protocol configuration for each transmission so that the accuracy of the RF fingerprinting diminishes. We demonstrate the effectiveness of our scheme through simulation and prototype experiments.

1. Introduction

Current era can be characterized by major proliferation of computation and communication devices in all aspects of life. Particularly the rapid advances in radio technologies have been transformative where the increased and versatile wireless connectivity has enabled networked solutions for many unconventional civil and military applications. Cyber–physical systems and Internet of Things (IoT) are examples of major developments towards the realization of smart cities. Nowadays, wireless links are used in major infrastructure, such as power grids, manufacturing facilities, residential buildings, etc. On the other hand, pervasive sensing and ad-hoc networking of smart devices have been attracting growing attention from the research and engineering community, motivated by applications like situational awareness, asset tracking, air-borne safety, digital battlefield, and border protection. However, the great flexibility of wireless networking comes at the cost of an increased vulnerability to security attacks and privacy violations; hence performance tradeoffs become necessary to sustain robust operation [1].

The broadcast nature of radio transmissions makes wireless networks more susceptible to attacks than their wireline based counterparts. Basically, an adversary can deploy antennas in the region of interest to eavesdrop on radio links and intercept all packet transmissions. In addition to threatening confidentiality, the intercepted packets could facilitate launching a wide range of attacks, such as packet replay, impersonation, data manipulation, etc. Pursuing packet encryption has been the conventional means for tackling such vulnerability. Although the use of encryption would safeguard the confidentiality and integrity of data and the anonymity of its source, packet encryption does not prevent an adversary from using the intercepted transmissions to conduct traffic analysis in order to uncover the network topology, and determine the roles that nodes play. To elaborate, an adversary can localize the sender of the intercepted transmissions, even if the packet is encrypted [2,3]. By correlating the intercepted frames from various nodes, the adversary can conduct flow analysis to determine the packet dissemination paths [4], or apply statistical analysis of the traffic intensity to identify critical nodes [2].

The threat of traffic analysis to wireless networks has been extensively investigated in the literature, where quite a few countermeasures have been proposed [2,5,6]. The main design goal of these countermeasures is to prevent the adversary from associating a sender with a receiver by provisioning anonymity, e.g., using pseudonyms, and avoiding handshake protocols. However, the effectiveness of anti-traffic analysis schemes will be dramatically degraded if an adversary can

* Corresponding author.
E-mail addresses: lwassil1@umbc.edu (W. Lalouani), younis@umbc.edu (M. Younis), ubaroudi@kfupm.edu.sa (U. Baroudi).

https://doi.org/10.1016/j.comcom.2021.04.007
Received 30 November 2020; Received in revised form 3 February 2021; Accepted 6 April 2021
Available online 20 April 2021

distinguish between nodes through other means such as RF fingerprinting. It has been shown that radio transceivers, even those built by the same manufacturer, exhibit some unique characteristics for the transmitted signal [7–13]. In essence, these unique characteristics become a radiometric signature for the device. An adversary could intercept transmissions and apply machine learning techniques to classify the features and differentiate between the various RF emitters. Thus, RF fingerprinting could identify the node's radio transceiver, and strengthen the adversary analysis. Countering such a fingerprinting threat is quite challenging. Given the granularity of the attack, circuit-level countermeasures are the usual means. However, as the industry is adopting standardized chipsets and protocol implementation, imposing hardware modifications is highly undesirable and provisioning protection using unconventional means would be needed.

This paper focuses on the exploitation of radiometric signatures as an enabler for launching attacks against wireless networks, and proposes a novel methodology for countering such a threat. We first investigate the accuracy of the RF fingerprinting by studying the various transmitter-specific features. We show that for accurate radiometric signature detection, the RF features used for device classification are mainly extracted from the modulation domain; we report on experiments with sample wireless protocols in 2.4 ISM GHz, namely Zigbee where contemporary machine learning algorithms are applied to associate the radiometric signature to the involved devices. We then highlight how traffic analysis attack models can leverage RF fingerprints to boost the attack success. Finally, we promote an innovative defense methodology using adversarial machine learning (AML). Based on such a methodology, we then devise two effective schemes for degrading the accuracy of RF fingerprinting and consequently nullifying its contribution to traffic analysis.

The first scheme leverages the capabilities of emerging radio transceivers in supporting multiple link layer protocols; our proposed techniques exploits the feasibility of switching among these wireless protocols in order to confuse the adversary about the modulation schemes and introduce high error in the classification process of the device-specific RF features. Our second scheme pursues distributed beamforming to introduce now radiometric signatures when the transmissions of more than one node are combined. The idea is to inject fake identities and confuse the adversary about the source of a transmission. In both schemes, AML techniques are employed to determine the protocol configuration used for each packet transmission in order to introduce the most classification error for the attacker. A key advantage of both schemes is that they do not require any changes to the underlying radio transceivers and the device hardware, and hence they can be adopted in a broad range of applications.

Our proposed countermeasures are validated through extensive simulation as well as using prototype-collected data. To the best of our knowledge, our work is the first to tackle possible malicious use of RF fingerprinting without imposing hardware modifications. Preliminary results involving link-layer protocols have been reported in [14]. This paper extends the scope by devising a countermeasure using distributed beamforming, and analyzing the intertwined application of protocol switching at the link and physical layers, and validating the performance of the link and physical schemes. The contribution of this paper can be summarized as follows:

- We characterize the use of RF fingerprinting as a means for attacking wireless networks and determine the features that enable accurate classification of radiometric signatures.
- We propose a novel methodology for Radiometric signature Exploitation Countering using Adversarial machine learning based Protocol switching (RECAP).
- We develop a novel RECAP-based scheme that exploits the support of multiple link-layer protocols to implement coordinated switching order among the available protocols to confuse the adversary.
- We develop a physical-layer RECAP based scheme that pursues distributed beamforming in order to introduce radiometric signatures to deceive the adversary about the transmitter and the number of nodes in the network.
- We validate the effectiveness of the proposed schemes through extensive simulation experiments and using data collected from prototype experiments.

The paper is organized as follows. The next section discusses related work in the literature. Section 3 summarizes the system and attack models. Section 3 focuses on RF fingerprinting and reports our findings through lab experiments. Section 4 shows how RF fingerprinting can be exploited by an adversary in conducting traffic flow and statistical signature analyses. Section 5 presents the proposed RECAP methodology and its application in switching link-layer protocols. In Section 6, a distributed beamforming based countermeasure is presented. The validation results are reported in Section 7 and the paper is concluded in Section 8.

2. Related work

Radiometric can be classified as location dependent and location independent. For example, the RSSI or angle of arrival at the receiver could serve as a signature for the transmitter assuming that the two communicating nodes are stationary [15,16]. Obviously such a type of radiometric is location dependent, is sensitive to the environment condition, lacks flexibility, and is prone to errors. On the other hand, location-independent radiometric relies on features related to the transceiver hardware. As pointed out earlier, variations among the transceiver characteristics enable the distinction among them where each will have a radiometric signature that can serve as an identifier. These characteristic variations are caused by the manufacturing process and do not hinder the transceivers from successful operation. Numerous characteristics such as power amplifier imperfections, clock offset, amplitude and phase errors, etc., have been explored in the literature [7,8]. Location-independent radiometric techniques fall into two categories based on the used characteristics, namely waveform-based and modulation-based. The former exploits time and frequency representation of the transmitted signals [17–19]. Meanwhile, modulation-based techniques utilize sampled I/Q data and are shown to be more robust [7–12].

Other than investigating exploitable signal features, published work on the radiometric signatures either studies the effect of channel conditions and receiver impairment on their detection [20–23], how to increase the device identification accuracy and robustness [12,17,24–28], simplifies the analysis by feature reduction [29,30], or explores their use in device authentication for both security and crime-forensics applications [31–33]. To yield accurate signatures, Peng el al. [12] improve the classification by factoring in the channel conditions in determining feature weights, while Bihl et al. [13] point out that phase based features are more important. Meanwhile, Baldini et al. [24] use multiple receivers to define "golden reference" in order to make the RF fingerprint more robust and less sensitive to the receiver circuit so that the radiometric of a node remains associated with such a node for all receivers. On the other hand, deep learning classifiers are employed in [25–28] in order to boost the accuracy and robustness of the RF fingerprinting process.

Radiometric signatures are pursued as evidence of illegal introduction of fake base-stations in cellular networks [31], and for detecting unauthorized flight of unmanned aerial vehicles [32,33]. We note that very few studies have considered radiometric manipulation. The approach of [34] is geared for forensics where a criminal is to be identified within a pool of suspects. The criminal is assumed to be able to exert control on the radio circuit to fool the investigator. RF fingerprints are also used for detecting unauthorized transmitters in a network where the legitimate nodes are known. Han et al. [35] uses AML to train a classifier for unauthorized nodes, while the deep learning model

of [36] identifies then using anomaly detection. Meanwhile, in [37] a radiometric is superimposed on a wireless transmission to enable authentication. Other work has assumed that adversary's awareness of the RF fingerprint of the targeted device and ability to accurately generate it [29,38–40]. Unlike such work, we do not introduce any changes to the radio circuit; instead we pursue protocol switching, guided by an AML methodology in order to prevent the exploitation of the radiometric in violating the anonymity of nodes and in launching traffic analysis attacks. To the best of our knowledge, our work is the first to tackle such a challenge.

Distributed beamforming can take multiple forms, of which amplify-and-forward cooperative relaying is of interest in the context of RECAP. The bulk of prior security-related work on amplify-and-forward cooperative relays has focused on channel secrecy and how to minimize information leakages for both known and unknown channel state information [41–43]. Generally, two security goals have been targeted in distributed beamforming [44], namely, (i) to lower the probability that an adversary detect the transmission [45,46], and (ii) to increase the level of noise at the adversary's receiver in order to prevent decoding intercepted messages [47–49]. RECAP simply leverages existing work and opts to achieve a different goal by introducing more radiometric signatures to give the illusion of increased node population and cause the traffic analysis to diverge. Particularly, RECAP assumes that the underlying distributed beamforming scheme does not require knowledge about the adversary's whereabouts [49].

Distributed beamforming has been exploited as a means for countering traffic analysis attacks [50,51]. The idea is to prevent an adversary from relating a communicating pair. Basically, a sender will recruit one or multiple relays and then cooperatively transmit with them to reach a destination that may be outside its radio range. To ensure clock synchronization among the cooperative transmitters, cross-layer optimization is proposed where features of the medium access control protocol are exploited [52]. Nodes are assumed to be unidentifiable by the adversary and transmissions cannot be decoded if intercepted, e.g., by using encrypted headers and payload. However, the perspective of identifying transmitters through RF fingerprinting has not been considered. As will be discussed in Section 4, disambiguating the senders and knowing the identity and number of nodes in the network enables the adversary to overcome the provisioned traffic analysis protection. RECAP strives to address such vulnerability by confusing the adversary about the radiometric signatures of existing nodes and introducing RF fingerprints through beamforming that constitutes fake nodes.

3. Accuracy of Radiometric Signature

To assess the effectiveness of RF fingerprinting and also check its dependency on the pursued wireless protocols, we have experimented with Zigbee and Bluetooth devices. The two protocols operate in the 2.4 ISM GHz Band, and are widely used in practice. The data is collected using a real-time spectrum analyzer that can handle radio frequencies up to 8 GHz with a maximum vector span of 36 MHz. It also easily captures continuous, intermittent or random signals generated in the close proximity of the antenna. The collected data is then preprocessed to extract all the important characteristics of the captured RF signals. The preprocessed data is used as input to two popular classifiers, namely SVM (Super Vector Machines) and KNN (K-Nearest Neighbors), both written in Python. All considered features, enlisted in Table 1, are from the modulation domain and extracted using the "digital demodulation mode" of the spectrum analyzer. The features in the table are ordered from the most effective to the least effective, based on the experiment results.

Here, we summarize the results for Zigbee devices; the experiments with Bluetooth have yielded consistent results and findings. Three groups of wireless motes operating under the Zigbee protocol have been used in the experiments: (i) 4 Xbee S2C wireless motes, (ii) 2 Xbee SMT Development Board (which also can be used as transmitters and receivers), and (iii) 10 Memsic IRIS Motes of the same model and manufacturer. The entire dataset was split into a training set and a testing set. The accuracy is calculated as $T_p/(T_p + F_p)$, where T_p is true positive, and F_p is false positive. Overall, the obtained classification accuracy ranges between 65%–84%. The experiments with Iris motes have demonstrated that I/Q origin offset could be helpful in identifying the correct node; nevertheless, the accuracy in this case stays at approximately 65% compared to 85% achieved with Xbee Motes. In addition, it has been observed that not all wireless motes of the same model and manufacturer are equally recognizable by the classifier, that is, two of the four motes used in Xbee experiments have shown an identification rate of average 85% throughout the experiments, while the identification of the other two motes has only reached an average accuracy of 70%.

We briefly report on how the selection of different radiometric features impacts the overall classification accuracy. The highest accuracy (~84%) has been reached with SVM when using only modulation error features, i.e., magnitude error, phase error and frequency error. Another observation is that each classifier (KNN and SVM) uses a different set of features to achieve the highest accuracy; KNN performs at best (70%) when the error vector magnitude is added to modulation error features, while for the same features SVM pull down the performance to 60%. In the same manner, the best feature used for SVM yields the worst accuracy (44%) in case of KNN. Overall, it can be stated that all motes can be correctly classified with the maximum accuracy of 84%. Based on the observations, the most effective features leading to the lowest misclassification rate are modulation errors, i.e., magnitude error, phase error and frequency error, and consequently are used in our performance analysis, as discussed in Section 7. Since the feature space is high-dimensional (more than two features are used for classification), SVM obtains more accurate classification results than KNN and hence the latter will not be considered in the balance for the paper. Overall, the experiment results have confirmed the effectiveness of radiometric signatures in identifying devices, which as we discuss in the next section can be exploited by adversaries in launching privacy and traffic analysis attacks.

4. RF fingerprinting exploitation

The major advances in wireless communication devices have led to the prevalence of networked system solutions for civil and military applications. In many of these applications, security is a core requirement and consequently the design and operation of the involved networks are to be concealed. For example, a networked set of sensor nodes could be deployed to operate unattended in a combat zone or along a border, where devices are to be camouflaged to avoid being captured and tampered with. Yet, the broadcast nature of wireless communications allows an adversary to eavesdrop in order to intercept transmissions. Although employing encryption will deprive the adversary from extracting relevant information from the intercepted packets, it cannot prevent traffic analysis [2]. The goal of the traffic analysis is to uncover the network topology and identify key players, such as active sources, data sinks, and critical relays that could be targeted by pinpointed attacks, e.g., radio jamming. Similar scenarios could be enumerated in the context of smart cities, internet of things, etc. Sustaining node anonymity, in terms of both identity and role, is the main defense strategy against traffic analysis. However, RF fingerprinting degrades the resilience of the network and diminishes the anonymity of nodes, and consequently makes the network vulnerable. In the following, we elaborate on the possible adverse effects of RF fingerprinting through two examples of traffic analysis attacks, namely, traffic statistical profiling and flow correlation.

Table 1
Radiometric features used for classification.

Feature	Description
Error vector magnitude	The vector of the magnitude difference between the ideal and measured phasors
Magnitude error	The difference in magnitudes between the ideal and measured phasors
Phase error	The angle between the ideal and measured phasors
Frequency error	The difference between the ideal and observed carrier frequencies, reflecting the amount by which the receiver's frequency had to be adjusted from the channel center in order to achieve carrier lock
I/Q origin offset	The distance between the origin of the ideal I/Q plane and the origin of the observed symbols

4.1. Traffic statistical profiling

When the network deployment area is physically inaccessible to the adversary, an effective means for conducting traffic analysis is to track the spatial distribution of transmissions. By intercepting transmissions, e.g., through highly sensitive antennas, and then estimating the location of transmitters, e.g., using trilateration algorithms, the adversary would form a statistical distribution of traffic intensity that can be further analyzed to uncover the network topology. Given the localization error and computational complexity, the analysis is typically based on a grid overlay of the deployment area where the number of transmissions per cell is used as an indication of the presence of important nodes within such a cell. For example, in sensor networks the vicinity (cell) of the base-station experiences high traffic volume and consequently the cell with the most transmission count could be where the base-station is located. Let N be the number of cells, and p_i be the probability at time t that a cell i contains the base-station. Then, the entropy of the system at time t is defined as:

$$entr_t = -\sum_{i=0}^{N-1} [p_i \times \log_2 p_i] \quad (1)$$

Initially, the probability for each cell will be $1/N$, which corresponds to the maximum entropy. With successful interceptions, the distribution of packets over the area changes and consequently cells' probabilities are adjusted. Such a process takes time and is still subject to errors. Consider the example scenario in Fig. 1. The cells with high transmission count do not correspond to the base-station. However, using radiometric signatures the adversary can estimate the node density and refine the analysis and/or identify highly active nodes, e.g., critical relays such as the one in cell #6, in order to distinguish the cells with high relaying rather than packet generation rates. Packet relaying will be more indicative of proximity to the base-station. Thus, RF fingerprinting could enable traffic analysis to converge rather fast.

4.2. Flow correlation attack

In this attack, the packet flow going to and out of the individual nodes is analyzed to determine where data from certain sources ends up being delivered. The objective is to identify the communicating parties over multipath routes. Such send/receive association enables the adversary of uncovering the role of the various network nodes and determining critical relays for successful network operation. Basically, the packet inter-arrival times are monitored and analyzed to estimate the traffic volume between node pairs and assess the portion of outflow from a node i reaching another node j. Such an attack scenario stays effective even if that path is intentionally extended with the incorporation of redundant relays [4]. In unattended setups, concealing the identity of nodes is a key mitigation measure for such correlated flow attacks since the adversary cannot accurately associate a transmission with a node without being in the vicinity, given the usually-high RF-based localization errors. By exploiting radiometric signatures, an attacker can succeed in identifying a transmission source and conducting flow correlation.

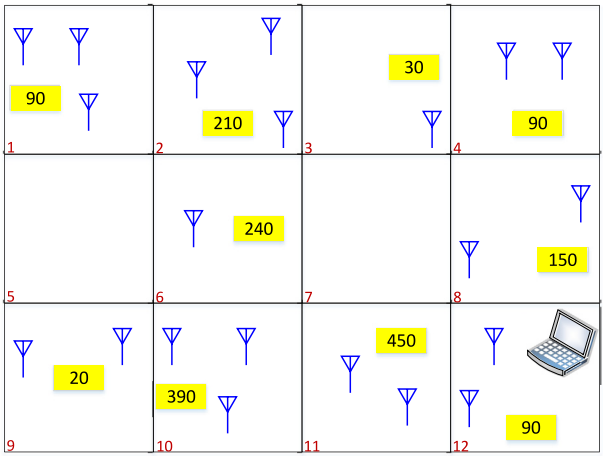

Fig. 1. An articulation of a traffic statistical profiling attack scenario. The number in each cell reflects the count of intercepted transmissions. An antenna denotes a node, while the laptop mimics the base-station (data sink).

5. System model and solution overview

Overall, lowering the radiometric accuracy will degrade the above-mentioned attacks and diminish their success. In this section we highlight some key assumptions about the node capabilities and network operation, and provide an overview of the RECAP methodology for countering RF fingerprint exploitation.

5.1. System model and assumptions

In this paper we consider multi-hop wireless networks that serve critical applications. The role played by the network nodes vary in the level of importance. An adversary strives to distinguish among the nodes and differentiate their roles so that targeted attacks could be launched. A node is assumed to know the location of the one- and two-hop neighbors, i.e., a transmitter knows the relative position of the receiver. This can be easily done through contemporary localization schemes and the exchange of two rounds of messages. Medium access collision is assumed to be mitigated by the underlying MAC protocol such that packet transmissions made by any subset of nodes will not collide. This can be achieved, for example, by a predefined time-based medium access arbitration or a dynamic contention-based reservation [53]. The network is assumed to have multiple link-layer options for establishing connectivity. Many commercial RF transceivers nowadays support multiple protocols. For example, the DIGI XBee3 wireless module supports multiple protocols, including Zigbee, DigiMesh, Bluetooth, and LR-WPANs [54].

RECAP exploits the use of distributed beamforming where multiple nodes cooperatively transmit a message in a synchronized manner. Fundamentally, cooperative wireless transmission employs multiple antennas so that the emitted RF signal can be steered in a certain direction with increased strength. The goal is generally to improve throughput, range, and link reliability. Unlike the case of having multiple antennas on the same node, e.g., Multiple Input, Multiple Output (MIMO), in distributed beamforming nodes with single antennas cooperate to form

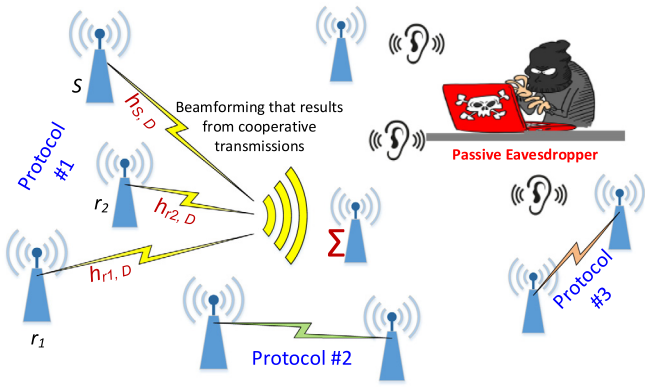

Fig. 2. Illustrating the network operation under RECAP, where multiple protocols are utilized and distributed beamforming is exploited in order to introduce radiometric signatures of non-exiting nodes.

a virtual multi-antenna system. Multiple nodes transmit simultaneously while factoring in the channel conditions and controlling the signal phase, so that all emitted signals are constructively combined at the receiver. To support distributed beamforming, the clocks of the involved nodes should be synchronized, which is typically needed for time-based MAC protocols and would not thus constitute an additional requirement for RECAP. It is assumed though that all nodes are willing to cooperate when requested.

Distributed beamforming allows the reduction of the transmission power of the source node S by $10log(|R| + 1)$ dB, where R is the set of cooperative relays [50]; however, this power savings for S does not characterize the total across the network as relays will incur overhead. The aggregated power usage for the transmission is dependent on the coordination overhead and data payload size. It has been shown in [50] that the overall transmission power for ideal signal reception signal η at the destination D while involving relays $r_j \in R$ is:

$$\begin{aligned}\eta_D(t) &\triangleq \eta_{S,D}(t) + \sum_{j=0}^{|R|-1} \eta_{r_j,D}(t) \\ &= \Re\left(A_S(t)\, w_{S,D} h_{S,D} e^{j(2\pi f_c t+\theta(t)+\varphi(t))}\right) \\ &+ \Re\left(\sum_{j=0}^{|R|-1} A_{r_j}(t) w_{r_j,D} h_{r_j,D} e^{j(2\pi f_c t+\theta(t)+\varphi(t))}\right) + n(t) \end{aligned} \quad (2)$$

where $\Re$ is the real operator that is used for complex baseband notation, $A(t)$ is the baseband pulse shape, w is the complex channel gain, h is the channel impulse response, f_c is the carrier frequency, $\theta(t)$ is a phase modulation term, $\varphi(t)$ is an aggregate phase shift term, and $n(t)$ represents the thermal noise present at receiver D. $\eta_D(t)$ is composed of two terms, the received transmission from the source S (i.e., $\eta_{S,D}(t)$) and the sum of the received transmissions from the $|R|$ relays, given by $\sum_{j=0}^{|R|-1} \eta_{r_j,D}(t)$. Fig. 2 illustrates the distributed beamforming concept with an example where nodes r_1 and r_2 serve as cooperative relays for S and the combined signals are received by D.

5.2. Approach overview

Fundamentally RECAP introduces more radiometric identities than the number of nodes in the network. The main goal is to confuse the adversary by injecting RF fingerprints that reflect fake nodes in the network. RECAP does so by exploiting protocols switching at the link and physical layers of the communication protocol stack. At the link layer, the node switches among the supported protocols by its radio transceivers. As discussed in Section 2, the RF fingerprint varies among the protocols and would point to the same source radio. Similarly, distributed beamforming mixes the emitted radio signals of two or more nodes; effectively the beamforming creates a new radiometric signature since the noise that constitutes the RF fingerprints is not additive. When applying beamforming to the collected experimental data of Section 3, the number of classes grew and the accuracy of the actual node RF fingerprints decreased by 10%. Assume that the radio transceiver of a node "x" supports P protocols and that N_x is the set of one-hop neighbors of x in the network. By applying RECAP, each transmission made by x can be in essence associated with $(P + N_x)!$ RF identities. This is quite powerful and for a network of M nodes and average node degree of μ, the number of distinct radiometric signatures in the network will be $M.(P + \mu)!$. To illustrate the level of confusion, for a network supporting 2 protocols and having an average node degree of 3, the number of distinct identities (nodes) exhibited through RECAP grows 120 times. Fig. 2 shows a simple illustrative scenario for how RECAP is applied in a network.

The interesting question is how a node selects the configuration of the next packet transmission, meaning (i) what link layer protocol it should use, and (ii) whether distributed beamforming is pursued or not, and if it is, which neighbors are to be engaged as relays. For determining how the next packet will be transmitted, our approach applies multiple criteria. First we enumerate all choices and employ AML to assess the impact of each choice on the adversary's RF fingerprinting analysis. Such AML analysis not only factors in classification error, i.e., loss function, but also the coverage range of the transmission. Basically, transmitting at a high power will increase the probability of interception, given the uncertainty about where the adversary's antennas are. Hence, distributed beamforming will be advantageous in that regard since the probability of intercepting the individual transmissions will be low and the combined beam corresponding to the fake signature will be high. Yet, increased participation in beamforming constitutes a risk since the involved relays will be in essence providing more data to the adversary if it happens to be nearby. Energy is another selection criterion where we consider the overhead for each transmission configuration choice.

Another important aspect is how the application of RECAP will be coordinated within the network. Basically, the receiver needs to be aware of the varying transmission configuration at the sender in order to be able to correctly receive the sent packet. For inter-node coordination, RECAP pursues a distributed and loosely-coupled scheme. A sender does not have to inform a receiver on a per packet level; instead a schedule for a batch of packets is shared. In other words, RECAP trades off latency and buffer space for decreased coordination overhead. A sequence of packets in a time epoch τ will be considered; for each of these packets the best configuration is selected. A node will broadcast the plan to its neighbors so that each of them knows what to expect. By knowing the level of neighbors' participation in the previous time epoch, each node factors that as neighbor's vulnerability and energy overhead, when scheduling the next sequence of packets. For example, assume node y is a neighbor of x. In a time epoch τ_i, node y served as a relay in 40% of the beamformed transmissions in the neighborhood. By knowing such heavy involvement, node x will limit the use of node y in time epoch τ_{i+1}.

6. Detailed RECAP methodology

In this section we present our RECAP methodology for decreasing the achievable accuracy of RF fingerprinting and confusing the adversary. RECAP does so by: (i) exhibiting multiple radiometric signatures for the same node through protocol switching, and (ii) introducing RF fingerprints with uncertain node association, through distributed beamforming.

6.1. Protocol switching

To confuse the radiometric identity of a node, RECAP injects data that negatively affects the classification algorithm that is applied to the intercepted transmissions. Such a process is often referred to as

poisoning and evasion, based on whether the training or test data is targeted, respectively. The general approach is called "Adversarial Machine Learning". In essence, adversarial machine learning methodically generates confusing data samples based on the actual data in order to result in misclassification. In the context of RF fingerprinting, applying AML will require means to manipulate the transceiver circuitry in order to produce the confusing data. We argue that such transceiver manipulation is complex and necessitates the use of custom-made radio circuits, due to the excessive cost, which is generally unwarranted and often blatantly unacceptable in most applications. Our approach avoids circuit level realization of AML; instead it pursues switching among multiple link layer protocols to achieve the AML goal. The support for more than one protocol does not necessarily require the incorporation of multiple radio transceivers aboard each node as many commercial products nowadays support multiple protocols, e.g. [54]. The objective of RECAP is to transmit the packet while introducing intentional perturbation into the RF fingerprinting data used by the classifier; it does so by mixing multiple protocols and selecting the nearest possible perturbation to the AML-derived values in order to make the radiometric inconclusive, meaning that the adversary cannot distinguish among the nodes with sufficient fidelity.

More formally, given a supervised classifier, the aim is to learn the model $f(x, \theta)$ from a labeled set of data $\{(x_i, y_i)\}$, where x and y can be in one of the k classes that represent the node identities. A machine learning model needs to predict the probability $P(y/x, \theta)$ using the loss function $L(x,y, \theta)$, where θ is the weighting vector of the classification parameters. AML opts to introduce a small perturbation, Δx, in the input to cause a large change in model output and maximize the loss, i.e., for δ>0: $\|\Delta x\| < \delta$, $\|f(x + \Delta x) - f(x)\| > \varepsilon$. Many techniques have been proposed in the literature for adversarial machine learning [55]. We use the fast gradient method for illustrating the operation of our approach and validating its performance. The fast gradient method utilizes the L2 norm bound ($\|\Delta x\|_2 \leq \epsilon$) and the derivative of the loss function with respect to the input, i.e., $\Delta x = \varepsilon . \frac{\nabla_x L(x,y)}{\|\nabla_x L(x,y)\|_2}$. By providing the adversarial sample $x_i^* = x_i + \varepsilon . \frac{\nabla_x L(x,y)}{\|\nabla_x L(x,y)\|_2}$, rather than x_i, the goal is to maximally diminish the classifier accuracy. However, in our case an AML technique is constrained in the data it can introduce since no physical layer alteration of the transmitted signals is deemed possible, which is a more practical assumption, given the dominant use of commercial-off-the-shelf transceivers and standard protocols. In other words, it is not possible to control the transmitter in order to provide x_i^*. Therefore, our approach sends the packet with the protocol that yields the closest value to x_i^*.

In summary, RECAP pursues protocol switching and employs AML to determine what protocol to use at a certain instance of time, specifically when sending some specific packets from a set of buffered packets. Again the AML technique cannot generate the exact transceiver imperfection that corresponds to the adversarial (poisoned) data, due to lack of physical layer control. Therefore, the transmission protocol for a subset of packets is picked such that the resulting features are highly discriminative to mislead the classification. Assuming a set of packets $\Psi = \{\psi_1, .., \psi_n\}$, and a set of supported protocols $P = \{p_1, .., p_m\}$, RECAP strives to determine for a node k the set of transmissions $T = \{(\psi_i, p_j)\}\ \forall\ 1 \leq i \leq n$, where $p_j \in P$, such that the accuracy of the radiometric signature of node k is minimized. This is accomplished in fast gradient by picking for each ψ_i a protocol p_j for which Δx_i is the least, i.e., smallest perturbation. Let Δx_i^j be the perturbation introduced by using protocol p_j for sending ψ_i. The set of T can be defined as follows:

$$(\psi_i, p_j) | \Delta x_i^j = min(\Delta x_i^1, \Delta x_i^2, \dots, \Delta x_i^m) \forall 1 \leq i \leq n \quad (3)$$

The intuition behind Eq. (3) is that the effect on the adversary's radiometric classifier is assessed when the packet is transmitted using each available protocol. The transmission with the least contribution to the adversary's classification accuracy is indeed favored and the corresponding protocol is used.

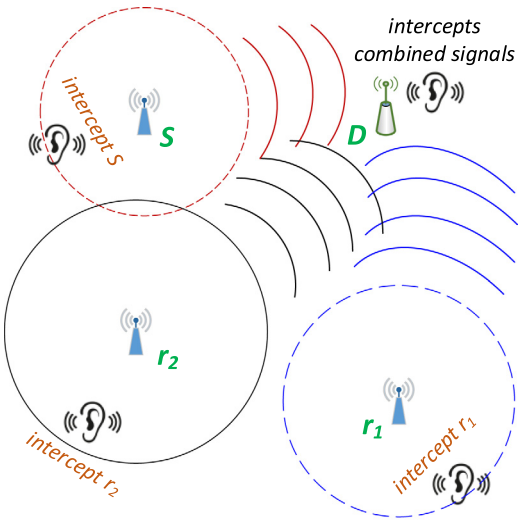

Fig. 3. The effect of cooperative transmission on the interception vulnerability of the transmission of the involved relays. Depending on the adversary's position (antennas) a transmission can be intercepted and associated with a relay, even if the combined signals reflect a different radiometric signature.

6.2. Distributed beamforming

As discussed in Section 4, distributed beamforming relies on cooperation among neighbors in transmitting the same message. As noted in Section 3, the combined RF signals in distributed beamforming exhibit a distinct RF fingerprint from the ones of individual participants. RECAP exploits such a feature to confuse the adversary by giving the illusion that some fake nodes are present in the network. Nonetheless, deciding to apply distributed beamforming and the selection of the cooperative relays are subject to tradeoff; specifically, the following factors ought to be considered:

Information leakage: When the eavesdropper position is not known, the longer the transmission range is the higher the probability of interception becomes. Such vulnerability can be assessed by the area covered by a transmission. Hence, when cooperative relays are engaged, they fundamentally run risk as their transmission can still be intercepted. Fig. 3 illustrates the issue. Nonetheless, the transmission power of each participant is usually much less than that when reaching the destination without beamforming. As stated in Section 5, there is $10log(R + 1)$ reduction in transmission power, and hence the risk is significantly less, yet it still exists. Generally, the node's and receiver's positions relative to the relays determine the required transmission power (range), and consequently the risk that a relay runs when taking part in a distributed beamforming.

Energy overhead: Generally distributed beamforming reduces the required transmission power for the source, yet at the expense of imposing overhead on the relays. Moreover, there is coordination overhead where a source should inform the relays what to send and precisely when. Hence, a source has to make a local broadcast to notify the relays and then transmits again the data along with them. Therefore, distributed beamforming will make sense only when reaching a destination that is more than one hop away from the source. Eq. (2) provides guidelines for how to factor the power in deciding to pursue beamforming given a set of relays. To amortize the overhead and also avoid the vulnerability to local interception, RECAP pursues coordination between a source and the neighboring cooperative relays at the level of a bundle, where the time and involved nodes are determined for each packet within the bundle and then the bundle information is shared with neighbors.

Node relaying load: The more the number of relays is, the more the number of fictitious radiometric identities becomes; as discussed in

Section 5, the availability of N relays enables the formation of up to $N!$ unique radiometric signatures corresponding to the various combination of cooperative transmitters. However, effectively every node would solicit the engagement of relays and if the selection is unregulated, the overhead could be uneven. To elaborate a node z could be selected by every neighbor to serve as a relay while another node y may stay mostly uninvolved. Since RECAP is applied autonomously by the individual nodes, there is no explicit status exchange and the load on the various relays is not updated. To overcome this issue, RECAP opts to balance the load across bundles. Basically, a node x will overhear the coordination messages from all its neighbors and infer the relaying load on each node in the neighborhood. Such load is factored in when node x selects relays in the next bundle. Obviously the node density will constrain the available relays. The effect of bundle size will be studied in Section 7.

6.3. Optimization and practical considerations

In practice, the receiver and the transmitter need to agree on a deterministic protocol of communication to avoid any mismatch between the protocol used for packet sending, and what is expected by the receiver. This issue can be tackled by either: (i) employing transmission preamble based on which the receiver can determine the protocol that the sender will soon use. Such preamble is usually small and is sometimes used by MAC protocols that support sleep modes [56]; (ii) using a control channel that is distinct from the data channel; and (iii) pre-agreeing on a specific protocol mix, i.e., protocol use frequency within a batch of packets, i.e., a bundle, and allowing packet ordering to make the protocol use pattern predictable. The third option achieves instantaneous agreement, and facilitates coordination for distributed beamforming; it is in fact the easiest to implement. Moreover, there will obviously be a trade-off between packet buffering (bundle size) and security. On the one hand, it is better to buffer more packets in order for the optimization formulation above to yield a better solution (i.e., expand the solution space). On the other hand, buffering will not only require storage but also impose packet delivery latency. Therefore, we expect the buffering aspect to be application dependent. In the next section, we study the implication of buffering on the performance of protocol switching in RECAP.

The operation of RECAP goes as follows. The time window size is determined for the network; such a window reflects the frequency at which the coordination among nodes takes place. Setting the window size is dependent on the data generation rate and in essence defines the frame size for the underlying MAC protocol; recall we assume a time-based medium access arbitration where each node reserves certain time slots to ensure collision-free transmissions. The receiver of a transmission is determined by the routing topology and is out of the scope of RECAP. There could be multiple bundles within a window depending on the window size; basically if the window size is significantly large buffering many packets would not be acceptable. Each node independently applies RECAP to determine the protocol to be used for each transmission within its packet bundle by applying the AML procedure discussed earlier in Section 4.1. Then, for each transmission the potential benefits of beamforming are evaluated.

The objective of RECAP is to select the subset of relevant players and protocols to orchestrate the transmission. Given the multiple unrelated factors to be considered in the beamforming decision, we apply fuzzy logic. Fuzzy-logic proved to be quite effective in mimicking the decision making process of humans by applying linguistic rules in a natural way. In essence, a fuzzy-logic based control can blend different parameters together to make a real-time decision. RECAP defines three levels for each decision factor, namely, high, medium, and low, and associates a decision for every combination. For example, when the load of a neighbor has been high, it is not involved as a cooperative relay more than 30% of the beam-formed transmissions in the current window. RECAP opts to select the most appropriate subset of relays among the neighbors using the following criteria:

Table 2
Sample fuzzy rules for selecting the cooperative relays.

Rule	Load	Energy	Distance	Probability
1	Low	Low	Close	High
2	Low	Low	Far	High
3	Low	High	Close	Low
4	Low	High	Far	Medium
5	High	Low	Close	Low
6	High	Low	Far	Medium
7	High	High	Close	Low
8	High	High	Far	Low

- *Load balancing*: A node that has many neighbors will be disproportionately overloaded compared to nodes with lower degrees of connectivity. RECAP tracks the node participation through overhearing. Basically, a node x counts how many times y transmitted and assesses the relative frequency. Normalization is conducted overall transmissions by all neighboring nodes and ranked as low, high, and medium, e.g., lower than 0.3, higher than 0.7 and in between. Such ranking will affect which fuzzy rule to be applied as shown in Table 2.
- *Energy overhead*: As discussed in Section 4, distributed beamforming can be beneficial in reducing the power of participating nodes. This, however, applies on the individual level and not collectively. In other words, the overhead for coordinating the synchronized transmission and picked relays may amortize the anticipating power reduction. RECAP associates an energy level for each combination of cooperative neighbors. Basically all combinations are considered and sorted according to the required energy; the sorted list is then partitioned into three sets reflecting low, medium and high energy requirements.
- *Relay proximity to the destination*: There is a trade-off here. Closer relay to the destination will allow reduced transmission power for the node and lower the probability of interception by the eavesdropper. Meanwhile, the further the destination is, the lower the adversary's ability of associating the packet sender and receiver, and consequently the higher the anonymity of the receiver. RECAP favors the subset of neighbors that are the furthest from the destination in order to degrade the potential of traffic analysis attacks.

Table 2 shows a sample of the fuzzy rules. Given the criteria, we will apply the fuzzy rules in order to determine the probability that a subset of neighbors will be used for beamforming. For example, a subset of nodes whose coordination imposes high energy overhead and are far from the destination should have a low probability of participation even if the involved nodes are lightly loaded. The higher the probability gets, the most likely the subset will be selected. However, applying beamforming constantly will overload the involved nodes and impose higher coordination overhead. Therefore, RECAP aims to balance such load by using a threshold for the probability that allows determining whether beamforming will be pursued or not.

RECAP is summarized in Algorithm 1. The algorithm consists of a loop over the buffered packets; for each of them the best protocol is picked based on AML, as discussed earlier. Such a process is reflected by the loop in lines 3–8 and its complexity is $O(m)$, where m is the number of protocols a node supports. Lines 11–19 are for determining the viability of beamforming and include a loop for checking the qualification of each subset of the node's neighbors for acting as cooperative relays. The fuzzy rules are applied to qualify the individual subsets. For an average node degree of μ, the computational complexity of such a loop is $O(2^{\mu})$. We note that in practice μ is not typically large; nonetheless in a dense deployment, a node can simply limit the number of neighbors that are considered in packet relaying. For example, a node can ignore neighbors that are further than itself from the packet receiver in order to conserve energy.

// RECAP execution on a node k
x : Input to the classier
y : Output to the classier, i.e., the node fingerprint (identifier in a finite set of nodes)
$L(x, y)$: Loss function which reflects the prediction error of the radiometric classifier
P : Set of protocols that node k can apply, with $P = \{p_1, .., p_m\}$
Ψ : Set of packets $\Psi = \{\psi_1, .., \psi_n\}$ to be sent by the node k
T : Set of packet transmissions $T = \{T_i \mid (\psi_i, p_j)\} \ \forall \ 1 \le i \le n$, where $p_j \in P$
N_k : The set of neighbors of node k
R_u^k : A subset of the neighbors of node i that can serve as cooperative relays $R_u^k \subseteq N_k \mid u \le 2^{N_k}$
r_i^k : a cooperative relay i for node k, i.e., $i \in N_k$
d_i : proximity of a relay i to the packet recipient
$E(R_u^k)$: Energy for cooperative transmission using the relay set R_u^k
$W(R_u^j)$: Weight for cooperative relay set R_u^k

1. For each $\psi_i \in \Psi$ // for each buffered packet determine the
2. $min = \infty$ // appropriate protocol
3. For each $p_j \in P$
4. $\Delta x_i^j = \varepsilon . \frac{\nabla_x L(x,y)}{\|\nabla_x L(x,y)\|_2}\Big|_{x=x_i^j}$
5. If min > Δx_i^j
6. α= j
7. endIf
8. endFor
9. $T_i = (\psi_i, p_\alpha)$ // p_α is best protocol for packet ψ_i
10. σ = empty set; $\omega = 0$ // Pick relays for beamforming
11. For each $R_u^k \mid u \le 2^{N_k}$
12. $Load(R_u^k) = \max_{i \in N_k} Load(r_i^k)$
13. Calculate $E(R_u^k)$ using Eq. (2)
14. Determine $W(R_u^k)$ by applying fuzzy rules
15. If $W(R_u^k) > \omega$
16. $\sigma = R_u^k$
17. $\omega = W(R_u^k)$
18. endIf
19. endFor
20. Beamformed transmission of T_i using σ
21. endFor

Algorithm 1: A Pseudo code summary of RECAP

7. Validation experiments

To validate the effectiveness of RECAP, we use experimental and synthetic data. The former is collected while experimenting with the Xbee and IRIS nodes, as discussed in Section 3. We have developed a simulation environment to generate synthetic data. We have considered two prominent machine learning algorithms, namely, SVM and Neural networks (NN). SVM is less computationally demanding than NN, and does not need a large training dataset. SVM suits sparse topologies and situations where the adversary can only gather a limited amount of data, e.g., in areas/networks with low traffic intensity. Meanwhile, NN performs better with high dimensionality data (i.e., with large number of features) and thus scales well for dense deployment, i.e., increased node degree. We evaluate the effectiveness of the protocol switching, AML strategies and beamforming in terms of the variation in the node's identification accuracy, the energy overhead, and the number of nodes (distinct fingerprints) perceived by the adversary. Due to the absence of any contemporary approach that tackles the same problem without any specific hardware for the manipulation of the quality of the packets transmitted, we compare our approach to the baseline case where no countermeasure is applied. The "sklearn" python library and the adversarial-robustness-toolbox from IBM [57], specifically the fast gradient method, have been used for generating AML data.

7.1. Simulation environment

In order to study the performance of our approach under varying frequencies of protocol usage, device counts and application of beamforming, we have developed a simulator using MATLAB to generate synthetic datasets. The simulator generates waveforms using Zigbee and Bluetooth Low Power (BLE) libraries of MATLAB. Although Zigbee and BLE are used in the evaluation, our methodology is generic and applies to other protocols. Imperfections in terms of amplitude and magnitude noise are generated for each node using uniform random distributions. The specific imperfections for node "x" are added to the RF transmissions when such a node sends a packet. Then, Gaussian channel noise is included in order to simulate the loss due to the communication. The receiver (adversary) measures digital modulation quality parameters in order to identify the transmitting node, as explained in Section 3. In the simulation, we track the error vector magnitude (EVM), magnitude error (MagErr), phase error (PhaseErr), and modulation error ratio (MER). These measurements can be represented by the points on the constellation diagram.

To collect these measurements, the adversary estimates the errors by comparing the received signals and those of an ideal noise-free transmission. The latter may be approximated using a filter such as Root Raised Cosine, Gaussian and Half Sine. In the simulation, we apply the raised cosine filter since it is frequently used for pulse-shaping in digital modulation and due to its ability to minimize inter-symbol interference. Once the ideal signal is determined, the vector of modulation error can be produced using the actual constellation points and the corresponding reference constellation points in every symbol period. The magnitude error, phase error and EVM are estimated using the following formulas [58]:

$$MagErr_{rms} = \sqrt{\frac{\sum_{i=0}^{i+N-1} \left(|S_i| - |R_i|\right)^2}{\sum_{i=0}^{i=N-1} |R_i|^2}} \tag{4}$$

$$PhaseErr_{rms} = \sqrt{\frac{1}{N} \sum_{i=0}^{i=N-1} (arg S_i - arg R_i)} \tag{5}$$

$$EVM_{rms} = \sqrt{\sum_{i=0}^{i=N-1} \frac{|S_i - R_i|^2}{\sum_{i=0}^{i=N-1} |R_i|^2}} \tag{6}$$

where S is the received signal and R is the estimated (ideal) reference signal. MER is another important feature that is considered in the simulation, but the error is calculated from the signal's average power. MER includes all imperfections including deterministic amplitude imbalance, quadrature error and distortion, while noise is random by nature. MER is measured in decibels (dB) and is defined by:

$$MER = 10Log_{10}\left[\frac{\text{Average symbol power}}{\text{Average error power}}\right]$$

For quadrature phase-shift keying modulation MER is calculated as:

$$MER = 10Log_{10}\left[\frac{\sum_{symbols}(I^2 + Q^2)}{\sum_{symbols}((\delta I)^2 + (\delta Q)^2)}\right] \tag{7}$$

where I and Q are the phase and quadrature components of the symbol vector, respectively. δI and δQ reflect the corresponding errors in these components.

Using the aforementioned features, the adversary applies machine learning algorithms, namely, SVM and NN. We have used the following parameters for SVM: RBF kernel with the coefficient is set to 1/number of features, the regulariser C equals 1.0, and the shape of the decision function is one versus one. For neural networks, we have employed the Rectified Linear Unit as an activation function with 15 hidden layers and automatic batch size. L-BFGS is used as a solver and the learning_rate_init, maximum iteration and momentum parameters are set to 0.001, 200 and 0.9, respectively. We have evaluated the effectiveness of

both protocol switching and unconstrained AML strategies in terms of the variation in the node identification accuracy. To nullify the effect of RSSI, we have set the power of the transmitter based on the proximity to the adversary and adjusted it by *10log(| R| + 1)* when distributed beamforming is applied, where *R* is the set of cooperative relays picked by RECAP.

When validating the performance of protocol switching alone, the density of nodes (transmitters) has been varied from 4 to 14. The protocol switching frequency has been variated from 0 to 50% by first assuming unconstrained packet buffering in terms of space and latency in order to grow the set of available packets for the AML-based selection strategy. Additional simulations have been conducted to capture the effect of restricted buffering. When applying beamforming, topologies with an average node degree of three are formed. A window size of 100 time slots is considered and the data generation rate for nodes is determined such that each node transmits multiple times. Basically, the window size constitutes the maximum data generation rate, which in turns is divided by the average number of neighboring nodes, i.e. 4 (node degree + 1). In addition, to the node fingerprinting accuracy, we study an additional metric for distributed beamforming, namely the number of exhibited node identities. Basically, we employ hierarchical clustering to show how many distinct identities the adversary may find when classifying the fingerprints.

7.2. Simulation results

Protocol switching: Fig. 4 reports the performance of SVM and NN when Zigbee is used as the primary protocol for communication and BLE is used for poisoning (confusing the classifier). Here we have considered 100 buffered packets and allowed RECAP to optimally assign a protocol to each packet so that the RF fingerprinting accuracy is reduced the most. Clearly, increasing the device density will diminish the accuracy as the anonymity set is larger and it becomes harder to distinguish among the involved device. It is important to note that the accuracy is high for both classifiers when no poisoning data is involved, which corresponds in the figure to "zero" mixed dataset. The accuracy decreases significantly when the percentage of poisoned data grows by having 20%–50% of the packets being sent using Bluetooth. Such performance confirms the effectiveness of our AML-based protocol switching mechanism in countering RF fingerprinting exploitation. It should be noted that it does not make sense for the poisoning data to exceed 50% since it will cause Bluetooth to be the primary protocol that determines the radiometric signature. Similar conclusions can be drawn when BLE is used as a primary protocol and Zigbee for poisoning, as shown in Fig. 5. A significant decrease in the accuracy is achieved by transmitting just 10% of the packet using Zigbee. However, the accuracy stabilizes and even grows as more packets are sent using Zigbee since the radiometric accuracy of Zigbee is found to be much higher than BLE, and given that packets for both protocols are fed to the classifier at training time.

Adversarial protocol switching: Fig. 6 reports the percentage of accuracy reduction as a function of the buffer size, when Zigbee is used as the primary protocol for a network of 4 devices. The plots in essence show how the AML-based protocol switching strategy is affected by packet buffering. The entry for "Pure Adv". reflects the case when a large packet volume (400 packets) is buffered and the best mix of Zigbee and BLE based transmissions of these packets are picked such that the accuracy is diminished the most. The other entries correspond to buffering 2, 4, 6, 8 and 10 packets. The ratio of poisoning data is also varied. The fast gradient method is deemed to be a very effective adversarial technique against the SVM classifier, which is evident from the results in Fig. 6(a). The accuracy is also dramatically decreased when the NN classifier is used (see Fig. 6(b)). Both figures illustrate the significant impact of using protocol switching even with limited buffering. To determine the packet mix, the ceiling of the poisoning

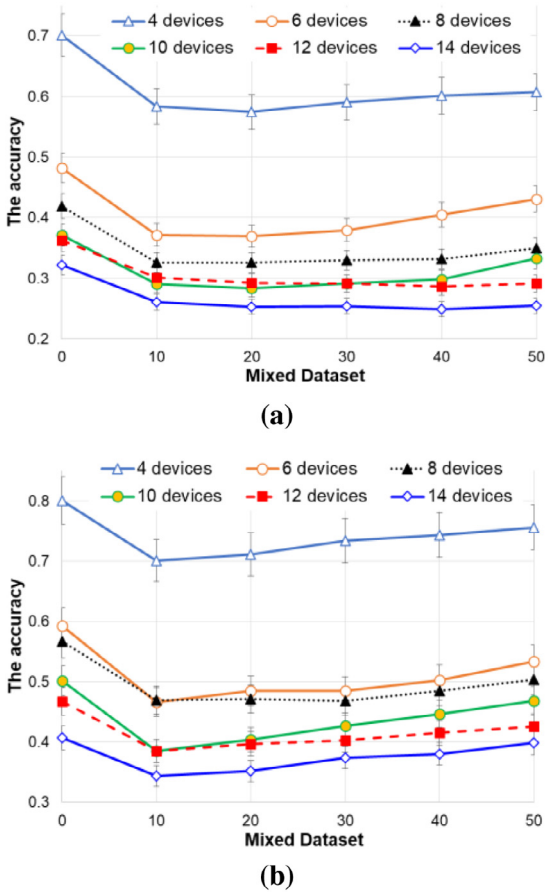

Fig. 4. RF fingerprinting accuracy of Zigbee when poisoned with BLE data while using (a) SVM, and (b) NN.

percentage of the buffer is used. That is for a buffer of 8 and 33.3% poisoning rate, 3 (rather than 2.33) secondary-protocol packets are included every 8 primary-protocol packet transmissions. Therefore, there is a slight leap in the 33.3% curve at a buffer of 8. Again, the higher the poisoning rate is, the more the accuracy diminishes. The same trends have been observed when BLE is used as the primary protocol (results are not shown due to space constraints).

Distributed Beamforming: Figs. 7 and 8 focus on the contribution of beamforming to accuracy reduction. We note here that the BLE data is used to poison the Zigbee transmissions when protocol switching is applied. Given the results in Figs. 4–6, the difference between SVM and NN is not notable and thus we report only the results when SVM is applied. As stated in the previous section, distributed beamforming creates RF fingerprints corresponding to the combinations of cooperating relays. Thus, a node could create fake radiometric signatures in its neighborhood. In fact, the diversity of the transmissions diminishes the classification accuracy of the RF fingerprints of the individual (actual) nodes in the network. When RECAP is not applied, some of the neighbors are randomly selected as relays. As demonstrated by the results in Fig. 7, distributed beamforming is more effective than protocol switching in that regard, despite the fact that the source node ends up transmitting more due to coordination with relays. The results indicate that the cooperative transmissions tend to confuse the classifier. RECAP, on the other hand, combines the advantages of both countermeasures. As seen in Fig. 7, RECAP diminishes the accuracy dramatically. Again the effectiveness of the countermeasures grows with the increased level of poisoning in the dataset mix.

Fig. 8 shows how many clusters the classifier yields when the various countermeasures are applied. In case of protocol switching,

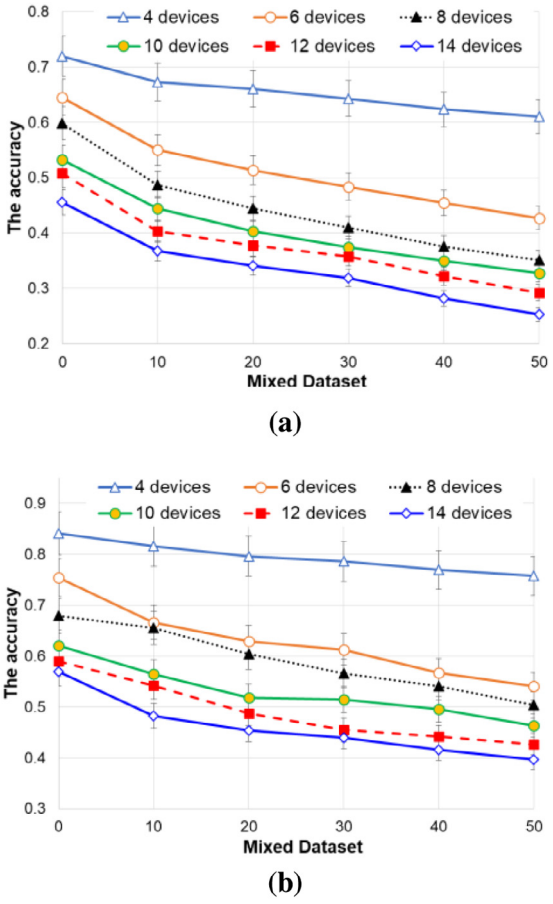

Fig. 5. The effect of device density and AML on BLE based radiometric while using (a) SVM, and (b) NN.

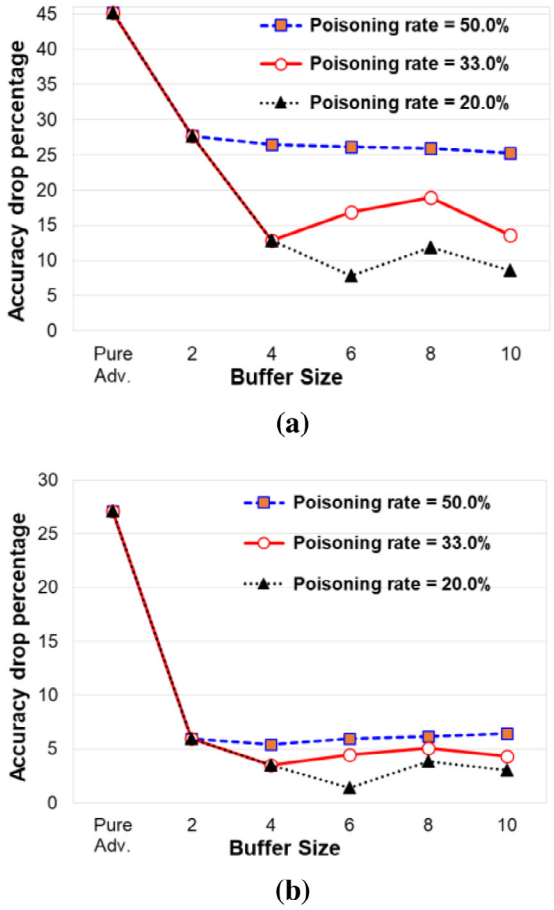

Fig. 6. Effect of packet buffering on accuracy when Zigbee is the primary protocol while using (a) SVM, and (b) NN.

the number of additional identities is proportional to the number of protocols and thus stays constant. Meanwhile distributed beamforming causes linear growth with the increased poisoning rate. RECAP sustains such growth while taking advantage of the protocol switching. We note that despite the superiority of distributed beamforming, it requires high level of network connectivity and consequently node density. Therefore, sole reliance on distributed beamforming would not suffice for all setups. RECAP strikes a balance where the number of clusters are moderately increased with infrequent application of distributed beamforming. We note that the small leap in the cluster count is due to the multi-criteria decision process. As discussed in Section 6.3, the fuzzy rules consider the energy overhead, load and proximity to the destination, and thus the application beamforming is somewhat constrained. Yet, considering Figs. 7 and 8 together clearly confirm the effectiveness of RECAP in protecting the network nodes and causing the classification accuracy to be very low.

Energy Efficiency: Fig. 9 reports the total energy consumed in packet transmissions by all nodes for the various configurations. We compare the cases of protocols switching, distributed beamforming and RECAP. For distributed beamforming, we report the results when the underlying protocol is Zigbee and Bluetooth. To calculate the energy we note the facts that: (i) Zigbee outputs 10 times more power than BLE, and (ii) the bit rate of Zigbee is 1–3 Mb/sec while it is 1 MB/sec for BLE. Given that the range of a BLE and Zigbee transmission is the same (originating from the same node and targeting the same receiver), we use generic energy units in our comparison by assuming the Zigbee transmit at 3 Mb/sec. Thus the energy per bit for Zigbee is 10/3 times that of BLE. For distributed beamforming we factor in the extra transmission for

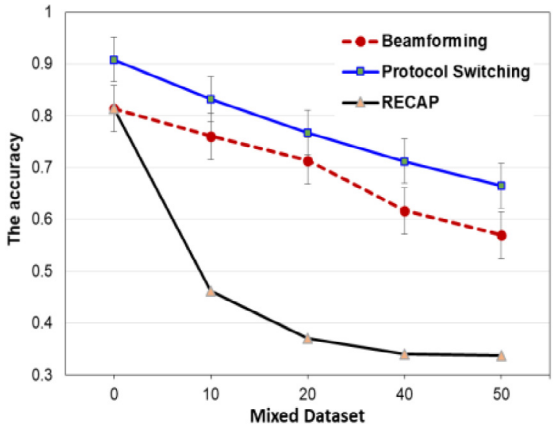

Fig. 7. Comparison of the accuracy reduction achieved by applying protocol switching, beamforming, and RECAP. The Zigbee's FR fingerprinting is here poisoned with BLE data while using SVM.

coordinating with the relays and also adjust the transmission power by a factor of $10Log(|R|+1)$, where R is the set of relays picked by RECAP. When RECAP is applied, relays are picked based on the algorithm in Section IV.C; on the other hand, when distributed beamforming is only applied, i.e., without protocol switching, the relays are randomly picked. We also note that the results for protocol switching in Fig. 9, are based on an equal share of BLE and Zigbee packets in the mix.

The results in the figure confirm the advantages of beamforming in reducing the transmission energy. BLE is more efficient due to its power

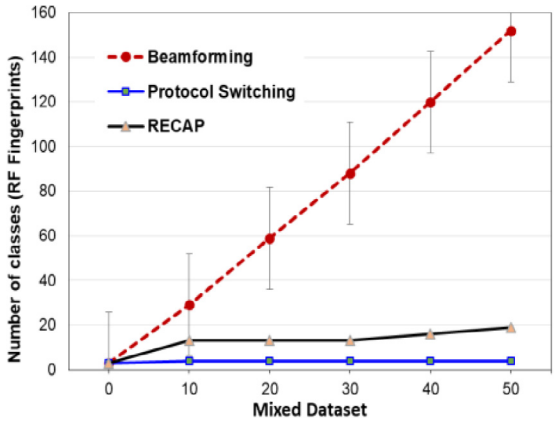

Fig. 8. The number of radiometric signatures when applying protocol switching; distributed beamforming and RECAP. A hierarchical cluster algorithm is used in the classification.

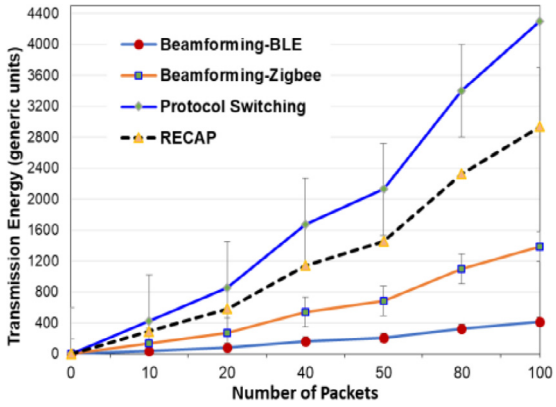

Fig. 9. Comparing the energy consumed in transmitting different sizes of packet bundles while applying RECAP, protocol switching, beamforming using BLE and Zigbee as the underlying protocol.

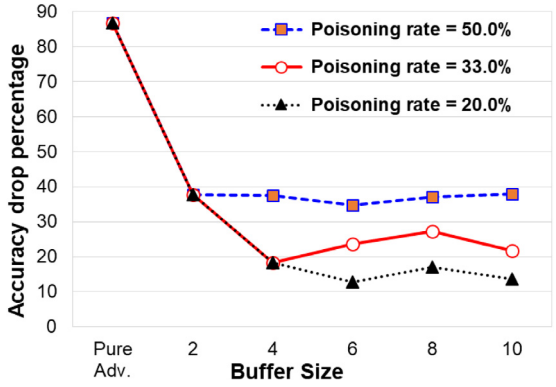

Fig. 10. Results when applying AML-based protocol switching using data collected for the Xbee and IRIS devices. Four nodes are assumed to be deployed. IRIS transmissions are used to poison Xbee data for the SVM classifier.

profile. Therefore, the beam-formed BLE is in the lead. Nonetheless, even for Zigbee distributed beamforming is 300% better than protocol switching in terms of consumed energy. Unsurprisingly, the RECAP curve lies between the curves of beam-formed Zigbee and protocol switching since beamforming is not applied all the time as indicated by Fig. 8. Figs. 7–9 collectively confirm the effectiveness of RECAP as a lightweight countermeasure against the exploitation of RF fingerprints.

7.3. Experiments results

We have assessed the effectiveness of our AML-based protocol switching strategy using the data collected while experimenting with Xbee and IRIS nodes. The results shown in Fig. 10 are based on four Xbee nodes, where the IRIS data are mixed with the Xbee data to confuse the classifiers. Three mixes are tried, namely, 50%, 33.3%, and 20%, reflecting the cases of sending an IRIS packet after every one, two and four Xbee transmissions, respectively. The characteristics of each packet are captured based on transmission using IRIS and Xbee. For the unconstrained scenario, all packets generated during the experiments are considered at the same time and each packet is associated with IRIS or Xbee transmissions such that the radiometric accuracy is maximally diminished. The results for the SVM classifier are shown in Fig. 10 under "pure Adv".

When packet buffering is constrained, the effect on accuracy declines since fewer options become available to the AML based protocol selection strategy; in such a case poisoning at a high rate is advisable. Again the leap for poisoning rates 20% and 33.3% is due to rounding, as discussed earlier in Section 6.2. Otherwise, increasing the buffer size has a nominal effect unless a large number of packets can be buffered. On the other hand, an increased poisoning rate is more advantageous, where a rate of 50%, i.e., equal split of packets among the two protocols, achieves about 40% reduction in accuracy. We note that similar trends have been observed when NN is applied. Finally, we note that the goal is to show the effect of AML on the radiometric accuracy and confirm the simulation results, although the IRIS and Xbee transmissions are not based on the same node.

8. Conclusions and future work

This paper has presented RECAP, a novel adversarial strategy in order to prevent the exploitation of RF fingerprinting to identify devices and conduct traffic analysis. We first have demonstrated the effectiveness of RF fingerprinting in determining radiometric signatures using machine learning techniques. We have further analyzed the accuracy of RF fingerprinting and highlighted how the accuracy affects the success of adversary attacks. Then, we have developed two novel countermeasures. The first is based on switching among preset communication protocols and employing adversarial machine learning to determine the protocol selection for a transmission so that the accuracy of the RF fingerprinting diminishes. The second mechanism pursues distributed beamforming in order to introduce fake radiometric signatures that further confuse the adversary. The validation results have confirmed the effectiveness of RECAP in diminishing the accuracy of the inferred RF fingerprints and the identification of the associate nodes. RECAP sets itself apart from competing approaches by its effectiveness in countering RF fingerprint exploitation without the need for any circuit-level support or device hardware modification. Such a distinct feature makes RECAP an attractive choice for a wide range of applications.

CRediT authorship contribution statement

Wassila Lalouani: Conceptualization, Methodology, Software, Validation, Formal analysis, Writing - original draft. **Mohamed Younis:** Conceptualization, Methodology, Formal analysis, Writing - review & editing, Supervision, Funding acquisition. **Uthman Baroudi:** Conceptualization, Methodology, Writing - review & editing, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors are grateful to Danila Frolov for his help in the data collection. Dr. Younis and Dr. Baroudi would like to acknowledge the support of the Deanship of Scientific Research at King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia under the grant IN171025.

References

[1] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE 104 (9) (2016) 1727–1765.
[2] N. Baroutis, M. Younis, Location privacy in wireless sensor networks, in: Habib Ammari (Ed.), The Philosophy of Mission-Oriented Wireless Sensor Networks, Springer, 2019.
[3] M. Mahmoud, X. Shen, A novel traffic-analysis back tracing attack for locating source nodes in wireless sensor networks, in: Proc. of IEEE Int'l Conf. on Comm., ICC 2012, Ottawa Canada, 2012.
[4] Z. Ye, F. Xinwen, B. Graham, R. Bettati, Z. Wei, Correlation-based traffic analysis attacks on anonymity networks, IEEE Trans. Parallel Distrib. Syst. 21 (7) (2010) 954–967.
[5] A. Proaño, et al., Traffic decorrelation techniques for countering a global eavesdropper in WSNs, IEEE Trans. Mob. Comput. 16 (3) (2017) 857–871.
[6] R. Manjula, R. Datta, A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs, Comput. Netw. 44 (2018) 58–73.
[7] Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities, IEEE Commun. Surv. Tutor. 18 (1) (2016) 94–104.
[8] N. Soltanieh, Y. Norouzi, Y. Yang, N.C. Karmakar, A review of radio frequency fingerprinting techniques, IEEE J. Radio Freq. Identif. 4 (3) (2020) 222–233.
[9] X. Guo, Z. Zhang, J. Chang, Survey of mobile device authentication methods based on RF fingerprint, in: Proc. of the IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Paris, France, 2019.
[10] V. Brik, S. Banerjee, M. Gruteser, S. Oh, Wireless device identification with radiometric signatures, in: Proc. of MOBICOM 2008, San Francisco, California, 2008.
[11] M. Ramasubramanian, C. Banerjee, D. Roy, E. Pasiliao, T. Mukherjee, Exploiting spatio-temporal properties of I/Q signal data using 3d convolution for RF transmitter identification, IEEE J. Radio Freq. Identif. (2021) in press. http://dx.doi.org/10.1109/JRFID.2021.3051901.
[12] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, Y. Yan, Design of a hybrid RF fingerprint extraction and device classification scheme, IEEE Internet Things J. 6 (1) (2019) 349–360.
[13] T.J. Bihl, K.W. Bauer, M.A. Temple, Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions, IEEE Trans. Inf. Forensics Secur. 11 (8) (2016) 1862–1874.
[14] W. Lalouani, M. Younis, D. Frolov, U. Baroudi, Protocol switching mechanism for countering radiometric signature exploitation, in: Proc. of the IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, 2020.
[15] R.D.A. Timoteo, D.C. Cunha, A scalable fingerprint-based angle-of-arrival machine learning approach for cellular mobile radio localization, Comput. Commun. 157 (2020) 92–101.
[16] J. Yoo, S. Park, Fingerprint variation detection by unlabeled data for indoor localization, Pervasive Mob. Comput. 67 (2020) 101219.
[17] M.M.U. Rahman, A. Yasmeen, J. Gross, Phy-layer authentication via drifting oscillators, in: Proc. of the IEEE Global Communications Conference, GLOBECOM 2014, Austin, TX, 2014.
[18] M. Köse, S. Taşcioğlu, Z. Telatar, RF fingerprinting of IoT devices based on transient energy spectrum, IEEE Access 7 (2019) 18715–18726.
[19] A.C. Polak, S. Dolatshahi, D.L. Goeckel, Identifying wireless users via transmitter imperfections, IEEE J. Sel. Areas Commun. 29 (7) (2011) 1469–1479.
[20] J.K. Becker, S. Gvozdenovic, L. Xin, D. Starobinski, Testing and fingerprinting the physical layer of wireless cards with software-defined radios, Comput. Commun. 160 (2020) 186–196.
[21] A. Al-Shawabka, et al., Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting, in: Proc. of the IEEE Conference on Computer Communications, INFOCOM 2020, Toronto, ON, Canada, 2020, pp. 646–655.
[22] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, J. Yu, A robust radio frequency fingerprint extraction scheme for practical device recognition, IEEE Internet Things J. (2021) in press. http://dx.doi.org/10.1109/JIOT.2021.3051402.
[23] S. Ur Rehman, K.W. Sowerby, C. Coghill, Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers, J. Comput. System Sci. 80 (3) (2014) 591–601.
[24] G. Baldini, R. Giuliani, C. Gentile, G. Steri, Measures to address the lack of portability of the RF fingerprints for radiometric identification, in: Proc. of the 9th IFIP International Conference on New Techn. Mobility and Security (NTMS), Paris, France, 2018.
[25] F. Restuccia, et al., DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms, in: Proc. of the 20th ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc'19), Catania, Italy, 2019.
[26] S. Mohanti, N. Soltani, K. Sankhe, D. Jaisinghani, M.D. Felice, K. Chowdhury, AirID: Injecting a custom RF fingerprint for enhanced UAV identification using deep learning, in: Proc. of the IEEE Global Communications Conference (GLOBECOM 2020), Taipei, Taiwan, 2020.
[27] Q. Wu, et al., Deep learning based RF fingerprinting for device identification and wireless security, Electron. Lett. 54 (24) (2018) 1405–1407.
[28] M. Kevin, S. Revay, G. Stantchev, B. Nousain, Deep learning for RF device fingerprinting in cognitive communication networks, IEEE J. Sel. Top. Sign. Proces. 12 (1) (2018) 160–167.
[29] D.R. Reising, M.A. Temple, J.A. Jackson, Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints, IEEE Trans. Inf. Forensics Secur. 10 (6) (2015) 1180–1192.
[30] J.L. Padilla, P. Padilla, J.F. Valenzuela-Valdés, J. Ramírez, J.M. Górriz, RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation, Measurement 58 (2014) 468–475.
[31] Z. Zhuang, X. Ji, T. Zhang, J. Zhang, W. Xu, Z. Li, Y. Liu, FBSleuth: Fake base station forensics via radio frequency fingerprinting, in: Proc, of the Asia Conference on Computer and Communications Security, ASIACCS '18, Incheon, Korea, 2018.
[32] M. Ezuma, et al., Micro-UAV detection and classification from RF fingerprints using machine learning techniques, in: The Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, 2019.
[33] Q. Yang, H. Qin, X. Liang, T.A. Gulliver, An improved unauthorized unmanned aerial vehicle detection algorithm using radiofrequency-based statistical fingerprint analysis, Sensors 19 (2) (2019) 274–295.
[34] A.C. Polak, D.L. Goeckel, Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion, IEEE Trans. Wireless Commun. 14 (11) (2015) 5889–5899.
[35] H. Han, et al., Radio Frequency fingerprint based wireless transmitter identification against malicious attacker: An adversarial learning approach, in: Proc. of the International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2020, pp. 310–315.
[36] S. Hanna, S. Karunaratne, D. Cabric, Open set wireless transmitter authorization: Deep learning approaches and dataset considerations, IEEE Trans. Cogn. Commun. Netw. 7 (1) (2021) 59–72, in this issue. http://dx.doi.org/10.1109/TCCN.2020.3043332.
[37] P.L. Yu, G. Verma, B.M. Sadler, Wireless physical layer authentication via fingerprint embedding, IEEE Commun. Mag. 53 (6) (2015) 48–53.
[38] S. Ur Rehman, K.W. Sowerby, P.H.J. Chong, S. Alam, Robustness of radiometric fingerprinting in the presence of an impersonator, in: Proc. of the IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017.
[39] O. Gungor, C.E. Koksal, On the basic limits of RF-fingerprint-based authentication, IEEE Trans. Inform. Theory 62 (8) (2016) 4523–4543.
[40] B. Danev, H. Luecken, S. Capkun, K. El Defrawy, Attacks on physical-layer identification, in: Proc. of the 3rd ACM Conference on Wireless Network Security, 2010, pp. 89–98.
[41] H. Wang, Q. Yin, X. Xia, Distributed beamforming for physical-layer security of two-way relay networks, IEEE Trans. Signal Process. 60 (7) (2012) 3532–3545.
[42] L. Dong, Z. Han, A.P. Petropulu, H.V. Poor, Improving wireless physical layer security via cooperating relays, IEEE Trans. Signal Process. 58 (3) (2010) 1875–1888.
[43] J. Xing, T. Lv, X. Zhang, Cooperative relay based on machine learning for enhancing physical layer security, in: Proc. of the IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 2019.
[44] S. Yan, X. Zhou, J. Hu, S.V. Hanly, Low probability of detection communication: Opportunities and challenges, IEEE Wirel. Commun. 26 (5) (2019) 19–25.
[45] L. Wang, G.W. Wornell, L. Zheng, Fundamental limits of communication with low probability of detection, IEEE Trans. Inform. Theory 62 (6) (2016) 3493–3503.
[46] B. He, S. Yan, X. Zhou, H. Jafarkhani, Covert wireless communication with a Poisson field of interferers, IEEE Trans. Wirel. Commun. 17 (9) (2018) 6005–6017.
[47] H.-M. Wang others, Artificial noise assisted secure transmission for distributed antenna systems, IEEE Trans. Signal Process. 64 (15) (2016) 4050–4064.
[48] W. Zhang, J. Chen, Y. Kuo, Y. Zhou, Transmit beamforming for layered physical layer security, IEEE Trans. Veh. Technol. 68 (10) (2019) 9747–9760.
[49] J. Kong, F.T. Dagefu, B.M. Sadler, Distributed beamforming in the presence of adversaries, IEEE Trans. Veh. Technol. 69 (9) (2020) 9682–9696.
[50] J. Ward, M. Younis, Increasing base station anonymity using distributed beamforming, J. Ad Hoc Netw. 32 (2015) 53–80.
[51] J.R. Ward, M. Younis, Cross-layer traffic analysis countermeasures against adaptive attackers of wireless sensor networks, Wirel. Netw. 25 (5) (2019) 2869–2887.

[52] J. Ward, M. Younis, A cross-layer distributed beamforming approach to increase base station anonymity in wireless, in: Proc. of the IEEE International Global Telecommunications Conference (GLOBECOM 2015), San Diego, CA, 2015.
[53] M. Hadded, P. Muhlethaler, A. Laouiti, R. Zagrouba, L.A. Saidane, TDMA-based MAC protocols for vehicular ad hoc networks: A survey, qualitative analysis, and open research issues, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2461–2492.
[54] https://www.digi.com/products/embedded-systems/digi-xbee/rf-modules/2-4-ghz-rf-modules/xbee3-zigbee-3.
[55] S. Qiu, Q. Liu, S. Zhou, C. Wu, Review of artificial intelligence adversarial attack and defense technologies, Appl. Sci. 9 (5) (2019) 909–937.
[56] Y.Z. Zhao, et al., A survey and projection on medium access control protocols for wireless sensor networks, ACM Comput. Surv. 45 (1) (2012) 7.
[57] https://adversarial-robustness-toolbox.readthedocs.io/en/latest/.
[58] F. Hong, B. Xin, Z. Xin, L. Ke, The numerical simulation and experiment research for measurement of error vector magnitude (EVM), Appl. Mech. Mater. 103 (2012) 199–204.