

RESEARCH ARTICLE

Rethinking Tag Collisions for Replay and Relay Attack Resistance in Backscatter Networks

HOORIN PARK¹, (Member, IEEE), AND WONJUN LEE², (Fellow, IEEE)

¹Department of Information Security, Seoul Women's University, Seoul 01797, Republic of Korea

²Network and Security Research Laboratory, School of Cybersecurity, Korea University, Seoul 02841, Republic of Korea

Corresponding author: Wonjun Lee (wlee@korea.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) funded by the Korean Government (Ministry of Science and ICT) under Grant 2019R1A2C2088812 and Grant 2022R1G1A1007263, in part by Korea University, and in part by the Research Grant from Seoul Women's University under Grant 2022-0103.

ABSTRACT Distinguishable physical layer features of radio frequency have the potential to serve as new fingerprints for authentication in backscatter networks. They have a definite advantage that backscatter tags do not have to run resource-intensive operations that commodity tags rarely implement. However, current physical layer authentication schemes impose substantial burdens on both service providers and users. Since physical layer features are highly susceptible to environmental factors, labor-intensive and time-consuming fingerprint library establishment is indispensable to make sufficient statistics for authentication. In this paper, we propose *TagDuet*, a collision-assisted authentication scheme that adopts an auxiliary tag to RFID systems, a typical type of backscatter networks, without the requirement of fingerprint library establishment. TagDuet places an independent backscatter tag in the proximity of a reader and utilizes the features in intended tag collisions to improve wireless security. Our phase cancellation decoding algorithm accurately decodes the collisions, which leads TagDuet fully compatible with the commodity RFID tags. TagDuet provides freshness, the paramount property to resist replay attacks, and robustness to relay attacks under FCC regulations for frequency hopping. We implement a prototype of TagDuet with commodity tags, evaluate the performance in randomized channels by the auxiliary tag, and demonstrate the resilience against replay and relay attacks.


INDEX TERMS Authentication, backscatter network, RFID, relay attack, replay attack, wireless security.

I. INTRODUCTION

Radio Frequency IDentification (RFID) has been considered as one of the most promising technologies for providing the Internet connectivity to various physical objects by attaching tiny tags. Especially, the use of passive RFID tags operating with a backscatter networking technology in the Ultra-High Frequency (UHF) band is continually growing. The backscatter networking technology offers a number of advantages including low cost, no battery requirement, relatively long read range, and fast data rate. These benefits make UHF RFID tags well-suited for a wide range of Internet of Things (IoT) applications such as object tracking [1], access control [2], [3], healthcare [4], inventory management [5], [6], Passive Keyless Entry and Start (PKES) systems [7], and

material identification [8]. According to IDTechEx [9], most of the growth in tag sales is expected to come from passive UHF RFID.

In recent years, unfortunately, there are increasing concerns about security issues in RFID systems [10] since the passive UHF RFID standard in the early days has paid little attention to security and privacy [11]. Amongst the issues, tag authentication is one of the most challenging security problems since passive tags have scarce and limited computing resources, which makes traditional authentication protocols hard to be applied. In practice, checking non-modifiable transponder ID in a passive tag has been used for tag authentication, but now it is known that a programmable tag impersonation device [12] can easily evade the TID check. To this end, a tremendous number of cryptographic authentication protocols have been proposed, and even the recently updated standard [13] supports tag authentication

The associate editor coordinating the review of this manuscript and approving it for publication was Nabil Benamar .

with flexible choices on cryptographic suites. However, only a few commercial passive RFID chips (e.g., NXP UCODE DNA, NTLab NT1025D) implement the limited number of cryptographic algorithms, likely due to additional hardware requirements and performance degradation (e.g., communication range, tag reading speed) [14].

Meanwhile, many research efforts have focused on so-called *Radio Frequency (RF) fingerprinting* for tag authentication, in which RFID readers try to extract distinguishable physical layer features of tag response signals. For example, a variety of physical layer features such as phase rotation, time interval errors, and power spectral density are used. Since these approaches rely on random hardware impairments of the analog circuitry components introduced even in the same tag manufacturing process [15], predicting and counterfeiting such features are extremely hard. One advantage of RF fingerprinting is little dependency on protocols and RFID systems, enabling ease of integration with existing insecure RFID systems or cryptographic tag authentication protocols toward multi-factor authentication.

However, a significant drawback of RF fingerprinting is environment-sensitivity. That is, it is unstable when the radio environment changes. Although the radio environment could be controlled in laboratory or manufacturing settings, practical RFID applications rarely achieve such controlled environments. In this context, some latest research efforts propose to utilize environment-independent physical features such as the signal difference in a pair of adjacent tags [3], [16], or persistence time which measures the diversity of a charging circuit indirectly [14]. Nevertheless, all the existing approaches require labor-intensive and time-consuming fingerprint enrollment processes to establish a fingerprint library of legitimate devices, which are too expensive for system scalability. For example, in [17], the authors take ten seconds to collect data for each device.

This paper explores a new way to utilize physical layer features for tag authentication named *TagDuet*, which overcomes the drawbacks mentioned above of RF fingerprinting approaches. That is, in TagDuet, no fingerprint library establishment for individual tags is required, but the utilized features are environment-independent. Furthermore, TagDuet does not require any communication protocol or tag hardware modifications. TagDuet generates intended tag collisions which block the eavesdropping inherently and uses the physical layer features of the collisions to provide resistance to replay and relay attacks. Our phase cancellation decoding algorithm cancels the impact of collisions accurately. Therefore, TagDuet can be compatible with either loosely coupled (e.g., as a separated listener [18]) or tightly integrated (in software-defined RFID readers [19], [20]) RFID systems.

The key idea of TagDuet is to deploy a backscatter device,¹ called *auxiliary tag*, in the proximity of an RFID reader and

¹A backscatter device is a computing device with a passive backscatter radio [21]. RF-powered computers (or computational RFID tags) [22] and passive RFID tags are representative examples.

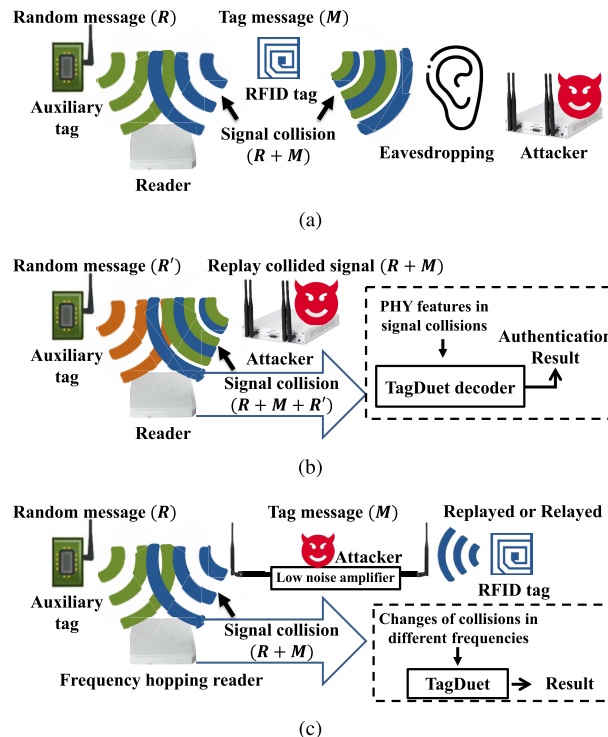


FIGURE 1. Overview of TagDuet: (a) An attacker mounts an eavesdropping attack to get a valid message M from a successful authentication process. However, the attacker obtains a collided signal, i.e., $R + M$, since the auxiliary tag transmits a random message continuously, denoted by R . (b) Though the attacker replays a valid signal from the previous authentication process, the TagDuet reader receives a collided signal, $R + M + R'$, with a new random message R' and can resist the replay attack. (c) The sole message M can be caught by an attacker outside the scope of authentication. With the auxiliary tag using frequency hopping, the TagDuet reader determines whether it is a truthful intended collision.

to make it backscatter an incident signal with a randomly generated message R during the authentication process of a passive RFID tag (with a message M), as shown in Fig. 1a. This incurs an intended signal collision ($R + M$) so that both conventional RFID readers and attackers cannot extract any meaningful message.

Meanwhile, a TagDuet reader can successfully decode the collided signal (i.e., extract M from $R + M$) to identify and authenticate the passive RFID tag *without prior knowledge about the random message R* . Furthermore, when the attacker replays the collided signal $R + M$ to attack tag authentication, the TagDuet reader can defeat the attack since the received signal contains the old message R as well as the current random message R' as shown in Fig. 1b. Worse, the message M can be solely replayed or relayed to make a valid signal collision ($R + M$) as shown in Fig. 1c. With FCC regulations for frequency hopping and the auxiliary tag, TagDuet investigates the changes of collided signals in different carrier frequencies to provide robustness to replay or relay attacks.

The main contributions of this paper are as follows:

- We present TagDuet, a novel physical layer authentication scheme compatible with existing RFID systems.

TagDuet generates intended tag collisions with an auxiliary tag and uses the environment-independent physical layer features of the collisions to provide robust protection against replay and relay attacks.

- We propose a new decoding algorithm, called *phase cancellation*, that successfully eliminates the effect of intended collisions. By incorporating the independent auxiliary tag, TagDuet can successfully identify a legitimate tag.
- We implement a prototype of TagDuet with a software-defined RFID reader and a single-board computer coupled with a backscatter switch. Also, replay and relay attacks are performed to defeat TagDuet. We conduct extensive experiments to demonstrate TagDuet's feasibility, reliability, and resiliency against the attacks.

The rest of this paper is organized as follows. We review existing research efforts on RFID tag authentication in Section II. Section III describes the motivation, and Section IV shows our adversarial model and challenges to be addressed for TagDuet design. The details of TagDuet design are introduced in Section V. We show TagDuet prototype implementation and evaluate its performance in Section VI. Finally, we conclude this paper in Section VII.

II. RELATED WORK

Since the original UHF RFID system of the Auto-ID Center was developed with a minimalist strategy, most passive RFID tags have been designed with severe computing and power resource constraints. Accordingly, conventional solutions for secure communications have rarely been applicable in UHF RFID systems, which leads to a broad range of security and privacy concerns [11], [23], [24], [25]. Amongst them, we specifically focus on research efforts on RFID tag authentication in twofold: *cryptographic algorithm-based approaches* and *RF fingerprinting-based approaches*.

In two decades, a lot of cryptographic algorithm-based approaches designed for passive RFID tag authentication have appeared. The great majority of research efforts try to reflect the resource constraints of RFID tags. They assume that either hash functions or physically unclonable functions are supported in the tags to perform cryptographic algorithms such as challenge-response mechanisms and symmetric encryption schemes [26], [27], [28], [29]. Unfortunately, the current UHF RFID standard [13] does not require such cryptographic functions. Hence, most of these approaches are not implemented on standard-compatible tags.

On the other hand, RF fingerprinting-based approaches try to utilize physical layer features. These approaches identify or authenticate passive tags based on physical characteristics that are observable in backscatter signals. The study in [15] shows the feasibility of UHF RFID tag identification by extracting the physical characteristics in a controlled environment. In [30], the authors propose an RF fingerprinting-based approach with the minimum power responses measured at multiple frequencies. Geneprint [31] utilizes a covariance of preambles and power spectral density for tag identification.

TABLE 1. Comparison between TagDuet and other authentication schemes. (Cryptographic algorithm-based: [26], [27], [28], [29]; RF Fingerprinting-based: [2], [3], [14], [15], [16], [30], [31], [32], and [33]).

	Crypto-based	RF Fingerprint-based	TagDuet
Hardware renewal	Required	Occasionally	Not required
RF fingerprint library	Not required	Required	Not required
Compatibility	Low	Medium	High

However, a recent study [16] reveals that the aforementioned approaches are not resilient to environmental changes.

In this context, more research efforts on RFID authentication utilizing physical layer features try to minimize the environmental sensitivity [16]. The studies in [2], and [32] use a collision signal as a kind of fingerprint of the backscatter devices. They authenticate a tag group by identifying the collision signal. Allowing only legitimate readers with information in the database to separate and decode the collisions can provide resistance to traceability and impersonation attacks. Hu-Fu [3] resists replay attacks by utilizing the inductive coupling feature of two tags as a fingerprint. However, since the inductive coupling occurs only at a distance of less than 4 cm, the authentication range is very limited severely, restricting the design space of backscatter network-based applications such as PKES systems [7]. Eingerprint [14] defines the notion of persistence time which can measure charging circuit diversity indirectly. RF-Rhythm [33] uses changes of phase information when the user taps on the RFID card. However, these approaches heavily rely on a time-consuming and labor-intensive fingerprint library construction phase.

In contrast, TagDuet does not require hardware or protocol modifications on commodity RFID tags as well as an exhaustive fingerprint library establishment process. Besides generating intended collisions, TagDuet blocks unauthorized eavesdropping inherently and prevents replay and relay attacks effectively, while maintaining compatibility simultaneously. Table 1 summarizes the characteristics of TagDuet compared to the current authentication schemes.

We note that prior work has also randomized the backscatter channels [34], [35] to block unauthorized eavesdropping. The difference, however, is that those efforts focused on blocking the passive eavesdropping using randomized reader's transmitting signals. Thus, they cannot prevent active eavesdropping outside the reader's interrogation range. On the other hand, TagDuet uses an auxiliary tag for its capabilities to not only prevent the eavesdropping, but also resist replay and relay attacks even if the attacker captures tag's signals outside the reader's range.

III. MOTIVATION

We are motivated by the fact that signal collisions can interfere with ordinary communications and decoding procedures. Specifically, the underlying idea of TagDuet is to utilize the collisions to improve security in backscatter networks.

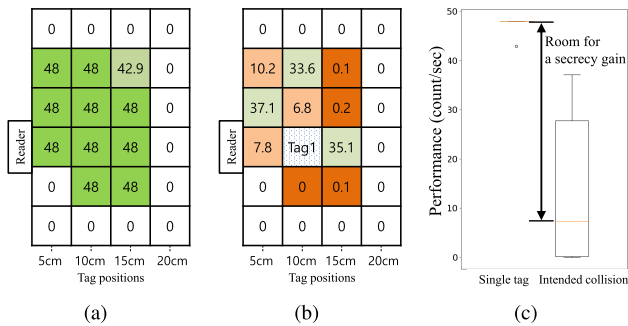


FIGURE 2. Impact of collisions on an RFID system: (a) The average number of identifications with a single tag and (b) two tags. (c) The signal collisions dramatically degrade the performance, but the difference between the performances shows room for a secrecy gain.

To validate the potential of collisions, we first explain experimentally how the collisions affect the RFID networks with a Commercial Off-the-Shelf (COTS) RFID system.

One of the novel ideas of TagDuet is leveraging intended signal collisions to prevent unauthorized eavesdropping, replay, and relay attacks. We conduct experiments with a COTS RFID system to determine the use of collisions on the RFID networks. The equipment used in each experiment is as follows: Host connected ThingMagic M6e RFID reader and two Alien ALN-9662 tags.

Fig. 2a shows the interrogation range of the system with 10 dBm transmit power. Each cell, 5 cm wide and 5 cm long, has the average number of tag identifications per second when a single tag located in the cell communicates with the reader. It shows that the tag responds 48 times per second. Even in an edge cell, the tag responds more than 42 times per second. To observe the impact of signal collisions, we modify a *Query* command parameter in the standard [13]. The command contains a slot-count parameter Q , which allows the receiving tag to pick a random value in the range $(0, 2^Q - 1)$. For multiple tags, choosing the appropriate Q can help avoid the collisions. Since TagDuet does not modify the communication protocol, the multiple tags respond according to the standard, with the exception of our auxiliary tag which always responds to the reader's excitation signals. If the tag picks zero, it replies immediately with a randomly generated 16-bit message for identification, called RN16. Fig. 2b shows the results when we place tag 1 at the center and set the value of Q as zero to force the collisions of two tags. The results show that the identification performance degrades dramatically by the intended collisions. As shown in Fig. 2c, there is a significant gap in the number of identifications between the single tag and the intended collisions of two tags.

Despite the degradation of identification performance, we may take another positive view from this phenomenon: *Can we make use of this gap for securer design of the system?* At this point, our observations can be interpreted that the difference can be room for a secrecy gain which can prevent an attacker from passive eavesdropping and resist more active replay and relay attacks. That is, *if the collision is generated intentionally and decoded successfully in the legitimate*

reader, it can be a new security primitive for RFID networks. In TagDuet, we use the secrecy gain for two functionalities: (1) inherent blocking passive eavesdropping and (2) evidence to detect replay and relay attacks.

IV. ADVERSARIAL MODEL AND CHALLENGES

Before using the potential of collisions for security, we describe an adversarial model to suppose the capabilities of attackers. Then, we present the challenges that TagDuet must resolve to overcome the threat models.

A. ADVERSARIAL MODEL

Our adversarial model includes three threat models that define passive eavesdropping, a naive replay attack, and advanced message-only attacks, respectively. We summarize the capabilities of the attacker as follows.

1) PASSIVE EAVESDROPPING

This threat model suppose the weakest attack. The attacker continuously performs as a receiver and records all the signals exchanged between the reader and tag. The attack aims to interpret the messages transmitted by the tag and use them in more powerful attacks, such as replay or relay attacks. TagDuet has inherent resistance to this attack by randomizing the channel similar to previous efforts [34], [35].

However, a MIMO eavesdropper [34] or collision recovery-enabled readers [36], [37] can decode the collided signals. Also, when the tag leaves the authentication area, even a normal reader can decode the signal by pretending to be a reader without interference (active eavesdropping). Therefore, TagDuet should provide robust resistance to further replay and relay attacks, even if the tag's messages have been exposed. Attacks based on active eavesdropping are described in advanced message-only attacks.

2) NAIVE REPLAY ATTACK

This model assumes an attack within the reader's interrogation range. The attacker records all signals transmitted by a target tag and replays them to a legitimate reader. The attacker want to deceive the reader by pretending to be a legitimate tag. Since the signals are always collided by an auxiliary tag, the attacker gets only collided signal as shown in Fig. 1b.

3) ADVANCED MESSAGE-ONLY REPLAY AND RELAY ATTACKS

In the attacks, for the purpose of obtaining authority, the attackers spoof the reader's command and get valid responses from a legitimate tag. The attacks are based on the captured signals without presence of the auxiliary tag. Since the tag owners are expected to be in various circumstances, the attacker can exploit active eavesdropping outside reader's interrogation range [25], [38].

Relay attacks are crucial threats on RFID systems. Many efforts try to defeat the relay attacks are classified as distance bounding protocols [39], [40], where distance bounding is

considered as a synonym of proximity check in the RFID literature. The protocols often use measured Received Signal Strength (RSS), Round Trip Time (RTT), and phase information [41]. However, an attacker can defeat the protocols with amplified relayed signals [7], speed-up computation [42], or incorrect phase information [43]. To make matters worse, inherent secrecy against eavesdropping in TagDuet and existing efforts [34], [35] cannot provide any protection against clandestine reading outside the reader's range. Then, the attackers obtain valid responses from a target tag and replay or relay them to get authority.

B. CHALLENGES

TagDuet design faces three challenges to be addressed to overcome the threat models.

Challenge 1: How to Interpret From the Collided Signals to the Legitimate Tag Messages

One of the goals is to establish an environment-independent authentication scheme without the RF fingerprint library of each user device. At the heart of TagDuet is the design of new security primitive that uses collision signals. Therefore, it is necessary to consider how to handle the collision signals. Especially, to maintain compatibility with the upper layer protocols, the message of the legitimate tag should be restored as it is transmitted. To achieve this, we present a new decoding algorithm, called *phase cancellation*, for collision signal processing when the legitimate tag's response collides with a random message from an auxiliary tag in the air.

Challenge 2: How to Make Sure That the Received Backscatter Signal is not a Signal Replayed by an Attacker. (Naive Replay Attack)

One of the major threats is the replay attack. Without accurate knowledge of the legitimate tag's message, the attacker attempts to pass the authentication by replaying the response signal in the previous successful authentication. At this time, Tagduet must ensure that the received collision signal is definitely the result of a collision by the legitimate tag and auxiliary tag without imposing any additional requirements on the legitimate tag.

Challenge 3: How to Verify the Received Backscatter Signal if an Attacker Obtains Only a Valid Message Outside the TagDuet's Communication Range and Replays or Relays it. (Advanced Message-Only Replay and Relay Attacks)

When the attacker commits replay or relay attacks with only the valid response, the reader receives a collided signal by an auxiliary tag. Since the received signal is the result of a collision by the replayed or relayed valid tag response and a random message of the auxiliary tag, it is very similar to the valid collision signal. Nonetheless, the TagDuet reader should reject the replayed or relayed signal.

V. TagDuet DESIGN

In this section, we elaborate on the design of TagDuet, which provides a new physical layer authentication scheme in backscatter networks.

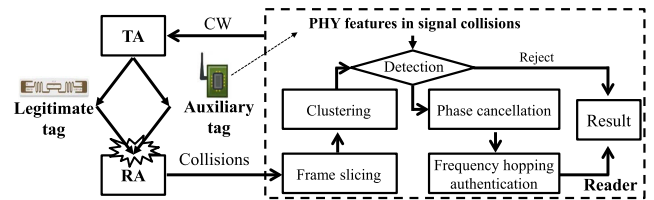


FIGURE 3. TagDuet design overview: The signal collision is received by the reader. The reader modules successfully cancel the impact of the auxiliary tag and decode the message of the legitimate tag. Moreover, TagDuet uses frequency hopping to provide robustness to replay and relay attacks.

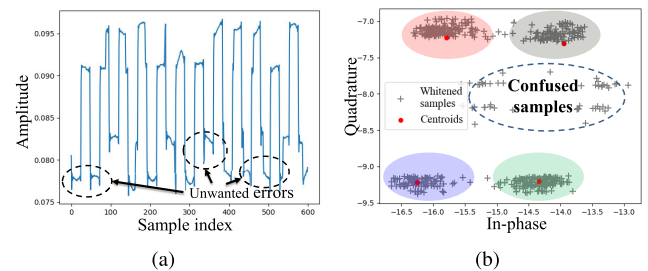


FIGURE 4. Collided signal clusters: (a) The amplitude of the received response in the time domain (b) in-phase and quadrature components of the whitened samples.

A. OVERVIEW

Before getting into the details, we introduce the modular overview of TagDuet design as shown in Fig. 3. The reader has two antennas, Transmit Antenna (TA) and Receiving Antenna (RA). The reader transmits Continuous Wave (CW) through the antennas and receives a collided signal from a Legitimate Tag (LT) and an Auxiliary Tag (AT). The legitimate tag represents a user, while the auxiliary tag is located close to the reader and is only controlled by a service provider.

The collided response is extracted through a frame slicing module. In the response, both the two tags (LT & AT) change their impedance as two states, high or low reflectivity (H or L). As a result, the collided response forms four clusters according to their states such that $(S_{LT}, S_{AT}) \in \{(L, L), (L, H), (H, L), (H, H)\}$. At this point, a clustering module analyzes centroids for the clusters. Each centroid indicates the state of tags, but there is insufficient information to identify the states.

Here, we analyze whether the legitimate tag and the auxiliary tag are truthfully involved in the received signal based on the physical layer features of auxiliary tag. Through the analysis, Challenge 2 is solved. The impact of auxiliary tag is removed through a phase cancellation decoding algorithm (Challenge 1). The reader has a message of the legitimate tag through FMO demodulation and checks if the result matches the stored data. Then, the reader changes its carrier frequency to obtain other collision signals. The multi-frequency authentication scheme provides robust resistance to the threats described in Challenge 3.

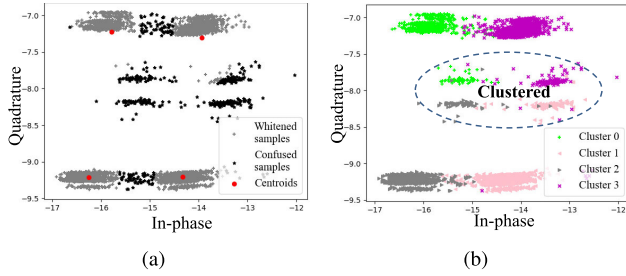


FIGURE 5. Clustering of the confused samples: (a) The confused samples are identified in black with distance-based probabilities and (b) classified according to the clusters of the adjacent samples.

B. CLUSTERING

A collided response is extracted by a frame slicing module based on the variance of signal amplitude within a certain time window. The baseband received response can be modeled at time instance t as follows:

$$y(t) = CW(t) + x_{LT}(t) + x_{AT}(t) + n(t), \quad (1)$$

where $CW(t)$ denotes the received CW from TA to RA, $x(t)$ is the backscattered signal by LT or AT, respectively, and $n(t)$ is complex noise. With the same oscillation of the reader device, $CW(t)$ can be presented as $ae^{j\alpha}$ where a and α are the amplitude and phase of the received CW, respectively.

The baseband backscattered signals are expressed by

$$x_i(t) = h_i b_i(t - \tau_i) e^{j(\theta_i + \alpha)} \text{ for } i \in \{LT, AT\}. \quad (2)$$

For each backscatter device i , h_i is a complex channel coefficient that depends on the channel of TA-to-tag and tag-to-RA, $b_i(t)$ is a binary number representing the state of each device, τ_i is a delay value before transmitting data, and θ_i is a phase shift from reflection coefficient.

The first challenge is to cluster the received response reliably. Based on Eq. 1 and 2, the response forms four clusters according to their bit-pair. The binary values of each backscatter device, $b_i(t)$, make square waves that contain unwanted noise such as harmonics and jitters during the state transitions due to slow capacitor charging. Fig. 4 shows an experimental result of signal collision by the two tags. In Fig. 4a, we plot the amplitude of the samples in the time domain. Dashed circles show some unwanted noise. Fig. 4b shows the centroids of clusters in red and whitened samples by the k-means clustering method. It shows that the confused samples cannot be clustered reliably. Although the existing work utilizes density-based clustering methods [36], [37], the confused sample problem caused by slow state transitions or harmonics has not been solved.

To achieve reliable clustering, we correct the clusters of the confused samples. First, we define a probability that the i -th sample belongs to cluster j as $Pb_{i,j}$ based on the distance between the sample and each cluster.

$$Pb_{i,j} = \frac{\frac{1}{\text{dist}(i,j)}}{\sum_j \frac{1}{\text{dist}(i,j)}} \quad \forall i, j, \quad (3)$$

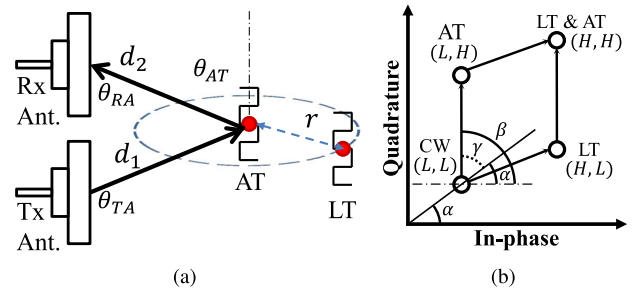


FIGURE 6. Phase model of TagDuet: (a) The signal traverses from TA-to-AT and AT-to-RA with phase rotations. (b) IQ diagram of the centroids in TagDuet.

where $\text{dist}(i, j)$ denotes the Euclidean distance between the i -th sample and the centroid of cluster j . We identify the confused samples such that $\max(Pb_{i,j}) < 0.5$, where 0.5 is a criterion to decide the most dominant cluster by majority. Generally, the samples are the median samples in cluster transitions. Thus, the confused samples are classified using the past and future samples that impact significantly the clusters to which they belong. More precisely, if there is a non-confused sample in the past and future samples, *i.e.* $\exists k, j$ such that $\max(Pb_{k,j}) > 0.5$, we set the cluster of the i -th sample as cluster j . We plot the result of confused sample clustering over a whole frame in Fig. 5a. After identifying the confused samples, the samples are classified based on the adjacent samples as shown in Fig. 5b. The clusters are used in the phase cancellation decoding to solely reconstruct the response of the legitimate tag.

C. PHASE CANCELLATION DECODING

The proposed phase cancellation decoding utilizes a physical layer feature of the auxiliary tag. The feature used in this part is the inherent phase rotation of the auxiliary tag. Since the position and orientation of auxiliary tag is fixed close to the reader, it is easy to obtain the phase information [44]. While the reader measures the phase, the result also includes additional phase rotations caused by radio signal propagation and antenna characteristics. Fig. 6a shows the phase model of TagDuet. As shown in Fig. 6b, the phase of the CW and the auxiliary tag, α and β , can be expressed as

$$\begin{aligned} \alpha &= \left(-\frac{2\pi}{\lambda} d_{self} + \theta_{TA} + \theta_{RA} \right) \bmod 2\pi \\ \beta &= \left(-\frac{2\pi}{\lambda} (d_1 + d_2) + \theta_{TA} + \theta_{RA} + \theta_{AT} \right) \bmod 2\pi, \quad (4) \end{aligned}$$

where λ is the wavelength; d_1 , d_2 , and d_{self} are the distances of TA-to-AT, AT-to-RA, and TA-to-RA; θ_{TA} , θ_{RA} , and θ_{AT} are the phase rotations due to the hardware characteristics of TA, RA, and AT, respectively.

In Eq. 4, the phase rotations, θ_{TA} , θ_{RA} , and θ_{AT} , are considered distinguishable static values that help to fingerprint the backscatter devices [45], [46]. According to the study in [8], the phase rotation by the tag θ_{AT} changes depending on the tag-attached material. In TagDuet, on the other hand, the

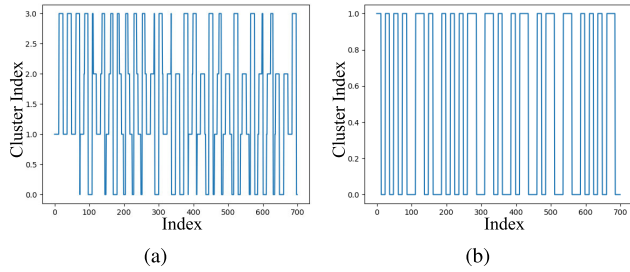


FIGURE 7. Reconstruction of the legitimate tag response: (a) Clusters transitions of the collision response and (b) reconstructed response of the legitimated tag.

attached material of AT is constant since it is only controlled by a service provider, resulting in stable phase rotation. Further, the positions and orientation of the antennas and the auxiliary tag are fixed, the measured phase information has a stable characteristic.

Based on the known static phase information of the auxiliary tag, TagDuet checks whether θ_{AT} is included in the centroids to verify that the response truthfully contains the signal transmitted from the auxiliary tag. However, since it is impossible to measure θ_{AT} directly, We use the difference of the measured phase values, $\gamma = \beta - \alpha$ in Eq. 4 instead of θ_{AT} . The centroid with the minimum difference from γ is affected by the AT. If the difference is bigger than the threshold, θ_{th} , it is regarded as an invalid response and rejected. That is, only responses including a centroid with γ value are regarded as valid responses. Otherwise, the authentication process will reject them. Then, TagDuet can prevent the replay attacks described in Challenge 2. The decision rule is as follows:

$$|min((\beta_i - \alpha) - \gamma)| \underset{Reject}{\overset{Accept}{\leq}} \theta_{th}, \quad (5)$$

where β_i is the measured phase of the i -th centroid.

Hereafter, we describe how to identify the clusters of the CW or AT and reconstruct the LT's response. The CW is estimated before the tag starts to transmit a message. Without loss of generality, we move the centroid of CW to the origin and get the phase information of other centroids. At this time, we suppose γ is already known to the reader. We identify the cluster affected by the AT with the minimum difference from γ . After the identification, TagDuet cancels the transitions by AT. With the clusters known, the decoding rule for TagDuet is as follows:

$$R[k] = \begin{cases} 1, & \text{if } C[k] \in \{C_{CW}, C_{AT}\} \\ 0, & \text{if } C[k] \notin \{C_{CW}, C_{AT}\}, \end{cases} \quad (6)$$

where k is the sample index, $C[k]$ is the cluster that the k -th sample belongs, and C_i means the cluster switched by $i \in \{CW, AT, LT, AT \& LT\}$. Fig. 7a shows cluster transitions of the collision response in the time domain. With the phase cancellation, the legitimate tag response can be reconstructed solely as shown in Fig. 7b.

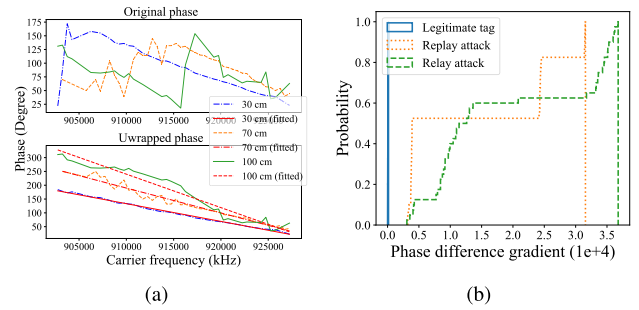


FIGURE 8. Received phase at different carrier frequencies: (a) Received phase from two tags at different distances and (b) phase difference gradient from a replay attack, a relay attack, and a valid authentication process.

After reconstructing the tag response, TagDuet starts to demodulate the FM0 symbols to solve Challenge 1. The demodulator calculates the intervals between adjacent cluster transitions. The FM0 modulation has transitions in every symbol boundary and the mid-symbol of a bit '0' [13]. The interval for representing a bit '1' is T with a tag symbol period T , and for a bit '0', there are two intervals with $T/2$. At this point, too short transition intervals are ignored since they are mostly due to the AT and noise. Then, we can determine with the legitimate tag message $b[n]$ with the following decision rule:

$$b[n] = \begin{cases} 1, & \text{if } 0.8T < t_d[k] < 1.2T \\ 0, & \text{if } 0.3T < t_d[k], t_d[k+1] < 0.8T, \end{cases} \quad (7)$$

where t_d is the array of transition intervals, and k is its index.

D. AUTHENTICATION USING FREQUENCY HOPPING

In Challenge 3, the attacker replays or relays the only legitimate tag message to the TagDuet reader. Since AT generates a signal collision with normal phase rotation, it can be regarded as a valid response in the phase cancellation decoding process.

To provide robustness to Challenge 3, TagDuet utilizes Frequency Hopping Spread Spectrum (FHSS) in backscatter systems. RFID systems usually incorporate FHSS in many countries since FCC 15.247 [47] regulates that all RFID readers operate across 50 channels ranging from 902 to 928 Mhz, and the average time of occupancy on any frequency shall not be greater than 0.4 seconds.

The heart of frequency hopping-based authentication is that the attacker only transmits the stored signal for replay attacks or the relayed signal from a distance, while the legitimate tag reflects the reader's signals of random frequencies. We use this fact to defend against replay and relay attacks.

Based on Eq. 4, the phase information of the backscattered signal depends on the wavelength λ . The wavelength is given by $\lambda = \frac{c}{f_c}$ where c is the phase velocity and f_c is the carrier frequency of reader. Then, we can express the phase

as follows:

$$\beta_i(f_c) = \left(-\frac{2\pi(d_i)}{c} f_c + \phi_i \right) \bmod 2\pi, \quad i \in \{AT, LT\}, \quad (8)$$

where d_i is the sum of distances (*i.e.*, TA-to-Tag_{*i*} and Tag_{*i*}-to-RA) and ϕ_i is the sum of stable phase rotations (*i.e.*, θ_{TA} , θ_{RA} , and θ_{Tag_i}).

Eq. 8 shows a linear function of f_c whose gradient depends on the distance between the tag and the antennas. We collect the phase values with the frequency hopping at different distances and show the results in Fig. 8a. We can observe that the phase varies with the carrier frequency and the gradient also depends on the distance. However, with the single tag information alone, it is difficult to distinguish whether the received signal is legitimate or under attack. In practice, a relayed signal which has a very long distance would have a wrapping phase value of 4π but it can be incorrectly interpreted as 2π in Eq. 8 and may show a low slope.

To this end, TagDuet uses the difference between β_{AT} and β_{LT} to resist replay and relay attacks. Before getting the phase difference, we unwrap the phase values to obtain a linear function. Since the response of each tag shares the carrier frequency of reader, the phase difference can be expressed by:

$$\Delta\beta(f_c) = \beta_{AT} - \beta_{LT} = \left(-\frac{2\pi(d_{AT} - d_{LT})}{c} f_c + \phi_N \right), \quad (9)$$

where ϕ_N denotes the difference between stable rotations, *i.e.*, $\phi_{AT} - \phi_{LT}$.

Eq. 9 shows that the gradient is proportional to the difference of distances between the reader and each tag. In a valid authentication process, d_{AT} is fixed, and d_{LT} is similar to d_{AT} to make the response message collide. This leads to a very moderate slope of $\Delta\beta(f_c)$. Conversely, when an attacker relays the valid response of LT from a distance, the relaying distance, d_{LT} , will be much greater than d_{AT} , *i.e.*, $d_{LT} \gg d_{AT}$. This leads to a large gradient of $\Delta\beta(f_c)$. For replay attacks, β_{LT} is fixed regardless of the carrier frequency. However, there are Carrier Frequency Offsets (CFO) between the reader and the attacker in practice. The CFO affects the measured phase values, and the phase difference values are widely distributed. Hence, if the gradient of the phase difference is above a threshold, β_{th} , the response is regarded as invalid and rejected. Fig. 8b shows the CDFs of phase difference gradients in legitimate cases, replay attacks, and relay attacks. TagDuet obtains the gradients of two or three samples with different frequencies. Based on the gradient, TagDuet can solve the problem described in Challenge 3. The decision rule is as follows:

$$|\nabla \Delta\beta(f_c)| \underset{\text{Reject}}{\overset{\text{Accept}}{\leq}} \beta_{th}, \quad (10)$$

where ∇f represents the gradient of a function f .

VI. PERFORMANCE EVALUATION

In this section, we demonstrate TagDuet with its prototype implementation. We first describe our implementation with

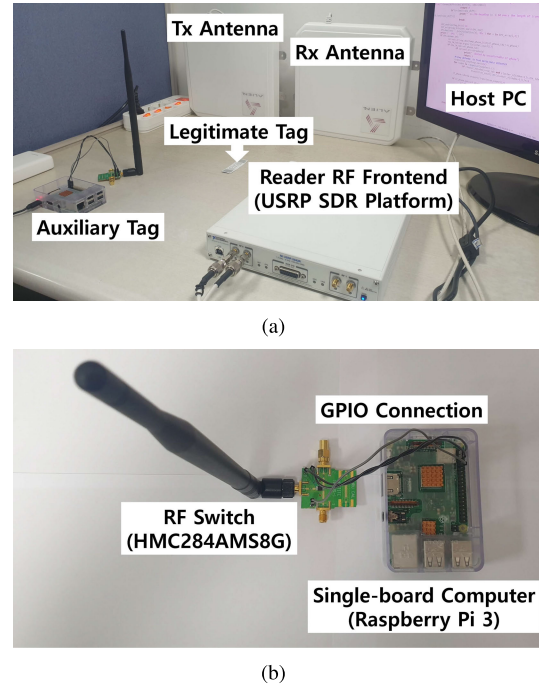


FIGURE 9. TagDuet implementation: (a) Testbed for the performance evaluation of TagDuet and (b) a prototype of auxiliary tag.

the experimental setup and then evaluate the performance of TagDuet in terms of three significant challenges to overcome.

A. IMPLEMENTATION

We develop a TagDuet prototype using one Software-Defined Radio (SDR) platform as a reader and one RF switch with a tiny Single-Board Computer (SBC) as an auxiliary tag.

1) READER AND TAG

As shown in Fig. 9a, a USRP SDR platform is employed for a reader's RF front. We choose two Alien ALR-8696-C as Tx and Rx antennas to communicate with a tag. The SDR platform is connected to a host computer that retrieves tag collisions for authentication. We use a modified GNU Radio-based Gen2 reader [48] as a baseline to compare the performance between a typical RFID reader and TagDuet. Alien ALN-9662 COTS tag is used as a legitimate tag.

2) AUXILIARY TAG

To generate tag collisions, we use an Analog Devices HMC284AMS8G RF switch evaluation board which has been widely employed for prototyping backscatter devices. The AT prototype has a 900 MHz hinged antenna and a 50 Ω termination on two front-ends for backscattering the incident signals. We control the AT with a Raspberry Pi 3 SBC. Fig. 9b shows the prototype of an auxiliary tag.

B. EXPERIMENTAL SETUP

We conduct real-world experiments with the TagDuet prototype to evaluate our design. As shown in Fig. 10, we choose

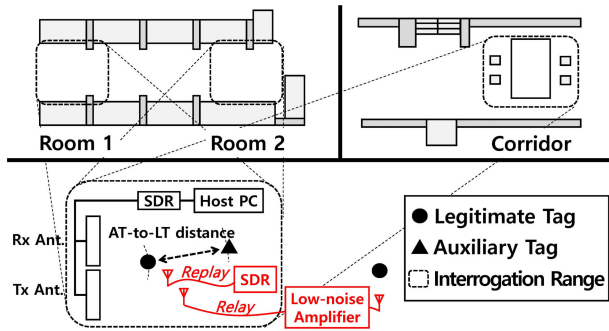


FIGURE 10. Experimental setup: Three different authentication areas and the placement of reader, LT, and AT in the interrogation range. An attacker launches a replay attack by using an SDR in the interrogation range, and a relay attack to the LT outside the range with a low-noise amplifier.

three different locations for the tag authentication area: Room 1, Room 2, and Corridor. Room 1 and Room 2 are different spots in the same room, while Corridor is a different area outside the room. One may point out that severe multipath fading or interference from other wireless devices from the indoor environment may affect the experimental results. Nevertheless, we show that TagDuet achieves exceptional performance in such conditions and works well in real-world scenarios.

In an authentication area, we run TagDuet and the typical Gen2 reader operation to read a legitimate tag located in the interrogation range. The size of the interrogation range is empirically set as 1.45 m × 1.45 m with acceptable decoding performance for SDR readers. We place reader Tx, Rx antennas, and LT in the interrogation range so that the reader sends a query to LT and receives the responses. AT is also placed to backscatter incident signals to cause tag collisions with the LT. With varied AT-to-LT distances, we investigate the performance of TagDuet and the typical reader. Note that the AT-to-reader and LT-to-reader distance is fixed as 1 m and 0.45 m, respectively.

In our threat model that corresponds to the challenges, an attacker has the capabilities to launch three types of attacks: naive $R + M$ replay, advanced message-only (M) replay, and relay attacks. We implemented these types of attacks with an additional SDR platform for replay attacks and low-noise amplifiers for relay attacks, respectively.

We assume that an attacker who has already acquired a collision signal $R+M$ or a sole M -only signal would replay them in the interrogation range. For replay attacks, we pre-record both types of signals and repeatedly inject them to TagDuet. The TagDuet reader should distinguish these invalid attempts from legitimate cases to perform reliable tag authentication.

For relay attacks, we suppose that the attacker equipped with low-noise amplifiers relays the signals between the reader and the LT outside the interrogation range. We employ two 20 dB gain low-noise amplifiers with two 2 m-long SMA cables to realize relay attacks. The signals are relayed in both directions: reader-to-LT and LT-to-reader. The reader-to-LT

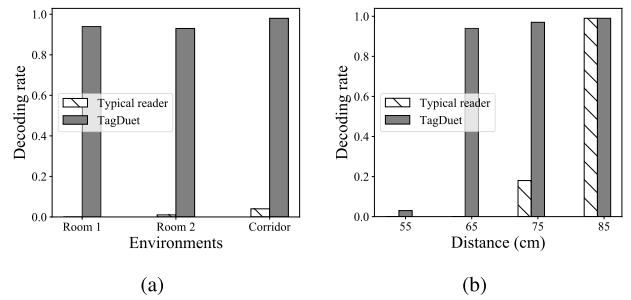


FIGURE 11. TagDuet decoding performance at different environments: (a) TagDuet shows exceptional performance regardless of its operating environments. (b) If the AT-to-LT distance is too close, LT’s response is indistinguishable from the noise floor. In contrast, if it is too far away, the signal power of LT will be strong, allowing the typical reader to decode the legitimate message.

relay amplifies the reader’s query signal and forwards it to the LT outside the interrogation range. The valid response of LT is also relayed to the reader in the reverse direction. Thus, the TagDuet reader has to reject these undesirable attempts that are very similar to the legitimate cases.

C. EXPERIMENTAL RESULTS

To validate the effectiveness of TagDuet, we evaluate our design in the aspect of the three major challenges mentioned above. First, we show that our phase cancellation decoding algorithm reliably decodes the responses from LT even if they are under the influence of the AT that introduces intended signal collisions. To demonstrate that Challenge 1 has been overcome, we use a decoding rate as an evaluation metric which is the number of correctly interpreted signals divided by the total number of given signals. The experimental result shows that TagDuet successfully decodes the signal collisions even under different environments. Second, we present the resiliency of TagDuet against naive signal replay attacks described in Challenge 2. Though the replayed signals have valid collisions, TagDuet successfully rejects them. However, as described in Challenge 3, if the attacker injects a legitimate message solely, the phase cancellation decoding algorithm accepts them correctly, *i.e.*, a false acceptance. Finally, we evaluate the performance of TagDuet with multi-frequency authentication. Even if the replayed or relayed signals are analogous to the intended collisions, TagDuet defeats the attacks effectively using the frequency hopping.

Here, we define the False Acceptance Rate (FAR) and False Rejection Rate (FRR) as the evaluation metrics with the following expressions:

$$cccFAR = \frac{(\# \text{ of accepted messages injected by an attacker})}{(\# \text{ of total messages injected by an attacker})}$$

$$FRR = \frac{(\# \text{ of rejected messages from the legitimate tag})}{(\# \text{ of total legitimate messages})}$$

1) TagDuet DECODING PERFORMANCE

We validate that TagDuet’s phase cancellation decoding algorithm keeps reliable performance in spite of environmental

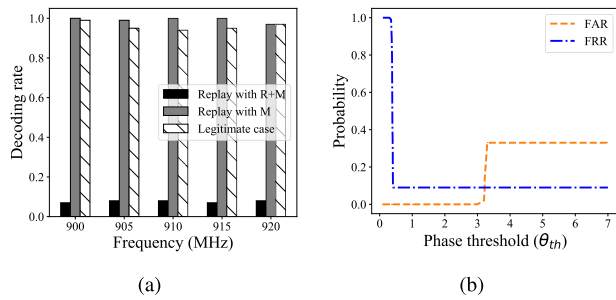


FIGURE 12. TagDuet performance against replay attacks: (a) Low decoding rate for $R + M$ replay attacks implies that TagDuet reliably rejects the naive replay attacker while it accepts message-only replay attacks falsely. (b) TagDuet achieves excellent performance with very low FAR and FRR against naive $R + M$ replay attacks.

changes. We also demonstrate the impact of AT-to-LT distance on TagDuet’s decoding rate. First, the decoding rate of TagDuet is compared to that of a typical reader across three different locations. As shown in Fig. 11a, the environments do not appear to present a significant challenge to the TagDuet decoding performance. On the other hand, a typical reader rarely decodes the responses due to the signal collisions introduced by the AT. This means that TagDuet provides reliable backscatter communications for the LT without the hindrance of environmental sensitivity.

Next, we observe the impact of distance between AT and LT on decoding rate. In Fig. 11b, we plot the decoding rates of TagDuet and a typical reader in different AT-to-LT distances. When the LT is 65 cm away from the AT, TagDuet decodes the responses successfully. However, a typical reader cannot read the response of LT due to tag collisions. This means that the distance is suitable for TagDuet since AT provides resiliency to potential attackers who may eavesdrop, record, and replay the response of LT. Note that TagDuet’s decoding rate also drops with decreasing AT-to-LT distance because the AT’s backscatter signal is relatively strong, and LT’s response is indistinguishable from the noise floor. As the AT-to-LT distance increases (reader-to-LT distance decrease), the decoding rate of a typical reader also starts to increase because the AT is unable to make substantial collisions due to the further distance. To summarize, TagDuet reliably and securely reads LT’s responses with desirable decoding performance regardless of environmental dependencies, which addresses and overcomes **Challenge 1**.

2) RESILIENCY TO NAIVE ($R + M$) REPLAY ATTACKS

We show that TagDuet thwarts a naive attacker who records a valid collision signal and injects it into the authentication area. In Fig. 12a, we plot TagDuet’s phase cancellation decoding rates for three cases: a legitimate case, a (naive) replay attack with a $R + M$ collision signal, and a (message-only) replay attack with an extracted single message M across five different carrier frequencies. We can find out that TagDuet effectively rejects the naive $R + M$ replay attacks. The main reason is that a naive collision signal $R + M$ would

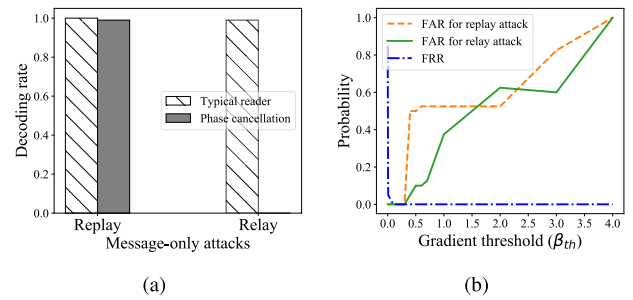


FIGURE 13. TagDuet performance against powerful replay and relay attacks: (a) High decoding rate for replay and relay attacks implies the false acceptance of decoding algorithm and the necessity of multi-frequency authentication. (b) TagDuet with multi-frequency authentication provides high accuracy with very low FAR and FRR against both replay and relay attacks.

collide again with a new random message R' from the AT. The received result $R + M + R'$ is easily distinguishable from the legitimate cases in TagDuet reader. However, TagDuet’s phase cancellation decoding algorithm still accepts message-only replay attacks since they are not distinguishable from legitimate cases whose received results would be very similar to the legitimate cases. Hence, TagDuet uses a multi-frequency authentication scheme to defend against these advanced replay attacks.

In Fig. 12b, we plot FAR and FRR under the naive replay attacks versus a phase cancellation decoding threshold parameter. TagDuet achieves almost zero FAR and 0.08 FRR at a phase threshold of 0.4. That is, TagDuet provides high resiliency by distinguishing naive $R + M$ replay attacks from legitimate cases. Note that FAR does not increase over 0.33 since most $R + M + R'$ signals have different characteristics compared to legitimate $R + M$ signals and are distinguishable in spite of liberal thresholds. We can confirm that TagDuet overcomes **Challenge 2** by reliably determining whether the received backscatter signal is legitimate or not with high accuracy.

3) RESILIENCY TO MESSAGE-ONLY (M) REPLAY/RELAY ATTACKS

TagDuet defends against more advanced message-only replay or relay attackers using the frequency hopping. Fig. 13a shows that message-only replay signals pass both phase cancellation and the typical reader. This means that the message-only replay signal is not simply distinguishable by employing the phase cancellation only. Thus, the necessity of multi-frequency authentication arises to detect these advanced replay attacks. Note that most relay attacks are prevented in the decoding step with a moderate phase cancellation threshold parameter. The root cause is that the relayed response is relatively noisier than the legitimate cases and harder to resolve intended collisions. Nonetheless, we relax this early rejection and forcibly pass to the multi-frequency authentication step to confirm the effectiveness of our design.

In Fig. 13b, we plot FAR of message-only replay, FAR of relay, and FRR versus phase difference gradient threshold

parameters. TagDuet shows highly accurate detection performance against the message-only replay and relay attacks. TagDuet achieves almost zero FARs against both types of attacks and zero FRRs in the range of gradient thresholds from 0.1 to 0.3. From the results, we conclude that TagDuet with multi-frequency authentication provides high resiliency to an attacker who can acquire a valid signal of LT's response and inject it by replaying or relaying. This confirms that TagDuet overcomes the remaining **Challenge 3**.

VII. CONCLUSION

This paper proposed a new physical layer authentication scheme, TagDuet, that adopts the backscatter device to RFID networks. The main advantage of TagDuet is that it does not require any communication protocol or tag hardware modifications and can be easily compatible with existing systems. Furthermore, while the existing physical layer authentication schemes require a time-consuming fingerprint library establishment step for each user individually, TagDuet does not impose such efforts. We built a prototype of TagDuet and conducted replay and relay attacks with an SDR platform. Although the replayed or relayed messages are valid, TagDuet can successfully defeat the attacks in the real-world experiments. We believe this work paves the way for collision-assisted security and can be adopted in other wireless networks to provide robustness against replay and relay attacks.

REFERENCES

- [1] M. Chen, J. Liu, S. Chen, Y. Qiao, and Y. Zheng, "DBF: A general framework for anomaly detection in RFID systems," in *Proc. IEEE INFOCOM*, May 2017, pp. 1–9.
- [2] H. Park, H. Roh, and W. Lee, "Tagora: A collision-exploitative RFID authentication protocol based on cross-layer approach," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3571–3585, Apr. 2020.
- [3] G. Wang, H. Cai, C. Qian, J. Han, S. Shi, X. Li, H. Ding, W. Xi, and J. Zhao, "Hu-Fu: Replay-resilient RFID authentication," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 547–560, Apr. 2020.
- [4] X. Chang, J. Dai, Z. Zhang, K. Zhu, and G. Xing, "RF-RVM: Continuous respiratory volume monitoring with COTS RFID tags," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12892–12901, Aug. 2021.
- [5] S. Qi, Y. Zheng, M. Li, Y. Liu, and J. Qiu, "Scalable data access control in RFID-enabled supply chain," in *Proc. IEEE 22nd Int. Conf. Netw. Protocols*, Oct. 2014, pp. 71–82.
- [6] J. Myung, W. Lee, J. Srivastava, and T. K. Shih, "Tag-splitting: Adaptive collision arbitration protocols for RFID tag identification," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 6, pp. 763–775, Jun. 2007.
- [7] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 2011. [Online]. Available: <https://www.ndss-symposium.org/ndss2011/relay-attacks-on-passive-keyless-entry-and-start-systems-in-modern-cars/>
- [8] B. Xie, J. Xiong, X. Chen, E. Chai, L. Li, Z. Tang, and D. Fang, "Tagtag: Material sensing with commodity RFID," in *Proc. 17th Conf. Embedded Networked Sensor Syst.*, Nov. 2019, p. 338.
- [9] D. Raghun, "RFID forecasts, players and opportunities 2019–2029: The complete analysis of the global RFID industry," IDTechEx, Cambridge, U.K., Tech. Rep. 700, 2019.
- [10] M. Burmester and B. de Medeiros, "The security of EPC Gen2 compliant RFID protocols," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, Jun. 2008, pp. 490–506.
- [11] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.
- [12] M. Lehtonen, A. Ruhanen, F. Michahelles, and E. Fleisch, "Serialized TID numbers—A headache or a blessing for RFID crackers?" in *Proc. IEEE Int. Conf. RFID*, Apr. 2009, pp. 233–240.
- [13] *Information Technology—Radio Frequency Identification for Item Management—Part 63: Parameters for Air Interface Communications at 860 MHz to 960 MHz Type C*, Standard ISO/IEC 18000-63:2015, Oct. 2015.
- [14] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Einger-print: Robust energy-related fingerprinting for passive RFID tags," in *Proc. USENIX Conf. Networked Syst. Design Implement.*, Feb. 2020, pp. 1101–1113.
- [15] D. Zanetti and B. Danev, "Physical-layer identification of UHF RFID tags," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Sep. 2010, pp. 353–364.
- [16] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive RFID," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 4, pp. 1–21, Dec. 2018.
- [17] P. Liu, P. Yang, W.-Z. Song, Y. Yan, and X.-Y. Li, "Real-time identification of rogue WiFi connections using environment-independent physical features," in *Proc. IEEE INFOCOM*, May 2019, pp. 190–198.
- [18] D. De Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: Towards distributed RFID sensing with software-defined radio," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2010, pp. 97–104.
- [19] N. Roy, A. Trivedi, and J. Wong, "Designing an FPGA-based RFID reader," *Xcell J.*, vol. 57, pp. 26–29, Mar. 2006.
- [20] E. A. Keehr, "A low-cost software-defined UHF RFID reader with active transmit leakage cancellation," in *Proc. IEEE Int. Conf. RFID (RFID)*, Apr. 2018, pp. 1–8.
- [21] A. Bletsas, P. N. Alevizos, and G. Vougioukas, "The art of signal processing in backscatter radio for μ W (or less) Internet of Things: Intelligent signal processing and backscatter radio enabling batteryless connectivity," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 28–40, Sep. 2018.
- [22] S. Gollakota, M. Reynolds, J. Smith, and D. Wetherall, "The emergence of RF-powered computing," *Computer*, vol. 47, no. 1, pp. 32–39, Jan. 2014.
- [23] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Inf. Syst. Frontiers*, vol. 12, no. 5, Nov. 2010, Art. no. 491505.
- [24] D. Zanetti, P. Sachs, and S. Capkun, "On the practicality of UHF RFID fingerprinting: How real is the RFID tracking problem?" in *Proc. Privacy Enhancing Technol. Symp.*, Jul. 2011, pp. 97–116.
- [25] F. Huo, P. Mitran, and G. Gong, "Analysis and validation of active eavesdropping attacks in passive FHSS RFID systems," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1528–1541, Jul. 2016.
- [26] G. Avoine, M. A. Bingol, X. Carpent, and S. B. O. Yalcin, "Privacy-friendly authentication in RFID systems: On sublinear protocols based on symmetric-key cryptography," *IEEE Trans. Mobile Comput.*, vol. 12, no. 10, pp. 2037–2049, Oct. 2013.
- [27] T. Li, W. Luo, Z. Mo, and S. Chen, "Privacy-preserving RFID authentication based on cryptographical encoding," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2174–2182.
- [28] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.
- [29] A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, and M. Yung, "End-to-end design of a PUF-based privacy preserving authentication protocol," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Sep. 2015, pp. 556–576.
- [30] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 6, pp. 938–943, Dec. 2011.
- [31] D. Ma, C. Qian, W. Li, J. Han, and J. Zhao, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," in *Proc. IEEE ICNP*, Oct. 2013, pp. 1–10.
- [32] H. Park, J. Yu, H. Roh, and W. Lee, "SCBF: Exploiting a collision for authentication in backscatter networks," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1413–1416, Jun. 2017.
- [33] J. Li, C. Wang, A. Li, D. Han, Y. Zhang, J. Zuo, R. Zhang, L. Xie, and Y. Zhang, "RF-Rhythm: Secure and usable two-factor RFID authentication," in *Proc. IEEE INFOCOM*, Jun. 2020, pp. 2194–2203.

- [34] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing RFIDs by randomizing the modulation and channel," in *Proc. NSDI*, May 2015, pp. 235–249.
- [35] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy, "RFID noisy reader how to prevent from eavesdropping on the communication?" in *Proc. 9th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Sep. 2007, pp. 334–345.
- [36] J. Ou, M. Li, and Y. Zheng, "Come and be served: Parallel decoding for COTS RFID tags," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Sep. 2015, pp. 500–511.
- [37] M. Jin, Y. He, X. Meng, Y. Zheng, D. Fang, and X. Chen, "Flip-Tracer: Practical parallel decoding for backscatter communication," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2017, pp. 275–287.
- [38] C. Shao, W. Jang, H. Park, J. Sung, Y. Jung, and W. Lee, "Phantom eavesdropping with whitened RF leakage," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 232–235, Feb. 2020.
- [39] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A framework for analyzing RFID distance bounding protocols," *J. Comput. Secur.*, vol. 19, no. 2, pp. 289–317, Mar. 2011.
- [40] A. I. Alrabady and S. M. Mahmud, "Some attacks against vehicles' passive entry security systems and their solutions," *IEEE Trans. Veh. Technol.*, vol. 52, no. 2, pp. 431–439, Mar. 2003.
- [41] I. Seto, S. Otaka, H. Yoshida, K. Nonin, M. Nishikawa, T. Kato, Y. Nito, H. Ishiwata, and T. Otsuki, "Sub-GHz two-way ranging based on phase detection for remote keyless entry systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9705–9720, Sep. 2022.
- [42] D. Celiano, "Overclocking proximity checks in contactless smartcards," M.S. thesis, Dept. Comput. Sci. Technol., Univ. Cambridge, Cambridge, U.K., Jun. 2018.
- [43] H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the security of carrier phase-based ranging," in *Cryptographic Hardware and Embedded Systems—CHES 2017*. Berlin, Germany: Springer, 2017, pp. 490–509.
- [44] P. V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. V. S. Rao, "Phase based spatial identification of UHF RFID tags," in *Proc. IEEE Int. Conf. RFID*, Apr. 2010, pp. 102–109.
- [45] L. Yang, P. Peng, F. Dang, C. Wang, X.-Y. Li, and Y. Liu, "Anti-counterfeiting via federated RFID tags' fingerprints and geometric relationships," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 1966–1974.
- [46] C. Wang, L. Xie, W. Wang, T. Xue, and S. Lu, "Moving tag detection via physical layer analysis for large-scale RFID systems," in *Proc. IEEE INFOCOM*, Apr. 2016, pp. 1–9.
- [47] *FCC Part 15 Radio Frequency Devices*, FCC document 15.247, Jul. 2021.
- [48] N. Kargas, F. Mavromatis, and A. Bleltsas, "Fully-coherent reader with commodity SDR for Gen2 FM0 and computational RFID," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 617–620, Dec. 2015.



HOORIN PARK (Member, IEEE) received the B.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, Republic of Korea, in 2011 and 2020, respectively. He is currently an Assistant Professor with the Department of Information Security, Seoul Women's University, Seoul. His research interests include RF-powered computing and networking, network security, and trusted execution environment design on the untrusted cloud.



WONJUN LEE (Fellow, IEEE) received the B.S. and M.S. degrees in computer engineering from Seoul National University, Seoul, Republic of Korea, in 1989 and 1991, respectively, the M.S. degree in computer science from the University of Maryland, College Park, MD, USA, in 1996, and the Ph.D. degree in computer science and engineering from the University of Minnesota, Minneapolis, MN, USA, in 1999. In 2002, he joined as a Faculty Member with Korea University, Seoul, where he is currently a Professor with the School of Cybersecurity. He has authored over 250 papers in refereed international journals and conferences and a book *Optimal Coverage in Wireless Sensor Networks* (Springer, 2020) (with D.-Z. Du). His research interests include communication and network protocols, wireless communication and networking optimization techniques, security and privacy in mobile computing, and RF-powered computing and networking. He is a fellow of the Korean Academy of Science and Technology (KAST). He has served on program and organization committees for numerous leading wireless and networking conferences, including IEEE INFOCOM, from 2008 to 2023, the PC Track Chair for IEEE ICDCS 2019, the Workshop Chair for IEEE ICDCS 2023, ACM MobiHoc, from 2008 to 2009, and over 148 international conferences. He has received numerous awards, including the IEEE Chester W. Sall Memorial Award, in 2018, the KIISE Gaheon Research Award, in 2011, the LG Yonam Foundation Overseas Faculty Member Award, in 2007, and the Best Teaching Award from Korea University, in 2005, 2009, and 2021, respectively. In 2019, his project "BackPlugged: Wearable-Optimized Ultra Low-Power Wi-Fi Networking With Plugged-in Backscatter Radio" was selected for 100 Outstanding National Research and Development Achievements by the Ministry of Science and ICT (MSIT) in South Korea. He is the President of the Korean Institute of Information Scientists and Engineers (KIISE), in 2023.

• • •