2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS) | 978-1-6654-0878-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICPADS53394.2021.00100

B-AUT: A Universal Architecture for Batch RFID Tags Authentication

Yinan Zhu*, Chunhui Duan†✉, Xuan Ding*, Zheng Yang*
*School of Software and BNRist, Tsinghua University, China
†School of Computer Science and Technology, Beijing Institute of Technology, China
Email: yn-zhu19@mails.tsinghua.edu.cn, duanch@bit.edu.cn, {dingxuan,yangzheng}@tsinghua.edu.cn
(✉ Corresponding author)

***Abstract*—RFID tags authentication is always a critical but challenging problem because only checking the EPC is vulnerable to counterfeiting attacks. Past works explore the unique backscatter signal features induced by tags' manufacturing imperfection as fingerprints, but fail to support simultaneous authentication for a batch of tags in practice, which is vital for large-scale RFID applications (*e.g.*, warehouse inventory). In this paper, we present a universal architecture, namely *B-AUT*, to simultaneously authenticate multiple tags even with the same EPC and pinpoint them, which is fully compatible with Gen2 standard and applicable to almost all tags' hardware fingerprints proposed in existing works. The workflow of *B-AUT* is threefold based on our novel algorithms. First, the extracted fuzzy fingerprint and EPC are jointly exploited to cluster raw data. Second, we extract the tags' fine-grained fingerprints for genuineness validation and obtain the invalid clusters. Third, we harness localization methods to match the invalid cluster to dubious tags and further conduct small-scale re-validation to pinpoint the counterfeit tags. We have implemented a prototype of *B-AUT* and evaluated it in extreme cases. Experiment results demonstrate that *B-AUT* can maintain nearly the same authentication accuracy as that of separate authentication and reduce the time overhead by 43.3%. Moreover, the pinpointing accuracy can reach as high as 92.8%, regardless of tags' total quantities or tag models.**

***Index Terms*—RFID, counterfeit attack, batch authentication, forged tags pinpointing**

I. Introduction

As one of the promising technologies in Internet of Things (IoT), radio frequency identification (RFID) gains increasing popularity in numerous applications, such as warehouse inventory [1]–[4] and unmanned retail [5]–[7]. In most RFID applications, commodity passive RFID tags that exploit backscatter communication are commonly used to identify items with unique digital identities due to their small-size, battery-free, low-cost and other advantages. Recently, the security threat of large-scale RFID applications has drawn much attention [8]–[11]. For example, adversaries may attach forged tags with eavesdropped valid tag ID to the fake products and stealthily substitute them for valuables stored in the warehouse, since the tags are firmly fixed on the items in general and thus cannot be easily torn out without leaving a trail. Therefore, it is vital to pinpoint the counterfeit tags in physical space among a wide range of tags for anti-counterfeiting.

Only checking the EPC (*i.e.*, tag ID) during authentication in the nascent stage is vulnerable to counterfeiting attacks (see Fig. 1) mentioned above. Besides, exploiting cryptographic

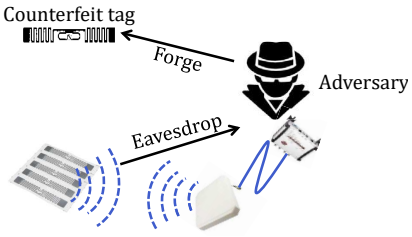

Fig. 1. Counterfeit attack on RFID tags

algorithms to encrypt the plaintext for avoiding eavesdropping is unaffordable and impracticable for most commodity RFID tags because these algorithms require extra hardware for high computation overhead and commodity tags cannot support them [12], [13]. To address it, recent works explore the tags' hardware differences induced by manufacturing imperfection and leverage unique signal features related to tags' hardware as the fingerprints to authenticate tags[1] [14]–[18]. However, these works cannot be applied to large-scale RFID applications, because of three weaknesses as follows:

- They cannot support batch authentication of multiple tags with the same EPC. Instead, authenticating each tag in sequence (*i.e.*, one by one) would incur extremely high time overhead and human efforts. For example, they fail to make the inventory of items at regular intervals for multiple times.
- They can only extract and validate all tags' fingerprints, however without knowing which tags are counterfeit ones matched to the invalid fingerprints. Thus, they are not able to pinpoint the counterfeit tags in physical space.
- Different types of tags' hardware fingerprints proposed in past works have their own pros and cons, with requirements of distinct RF devices respectively, *e.g.*, Butterfly needs software defined radios (SDR) and EingerPrint needs readers to conduct extra Gen2 commands [19]. There lacks a universal architecture that can apply to different scenarios.

To overcome the above limitations and achieve batch tags authentication, there exist two challenges: (1) before authenti-

[1]They actually focus on applications only authenticating a single tag at a time (e.g., entrance check), instead of practical multiple-tags scenarios.

2690-5965/21/$31.00 ©2021 IEEE
DOI 10.1109/ICPADS53394.2021.00100

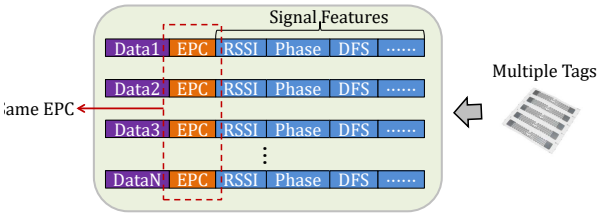

Fig. 2. The challenge of classifying data with same EPC

cation, it is hard to distinguish which sets of raw data collected from multiple tags' backscatter signals belonging to the same tag (see Fig. 2) because each tag always has more than one set of raw data during collection and multiple counterfeit tags may carry the same EPC as legitimate tags so that it is infeasible to classify data on the basis of EPC[2]; (2) after authentication, the matching relationships from invalid fingerprints to forged tags are ambiguous (see Fig. 3) because the signal features of all tags are collected together. Even though we scan each tag's EPC, the challenge still exists. Also, utilizing the timestamps of fingerprint data is unable to address this challenge due to the random backoff in the anti-collision mechanism of commodity tags [22]. Consequently, it is hard to match invalid fingerprints to corresponding counterfeit tags and further pinpoint them.

In this paper, we present the first universal architecture for batch tags authentication, namely *B-AUT* to simultaneously and precisely authenticate multiple tags and pinpoint the counterfeit ones, without any modifications on EPC-global Gen2 standard or RFID devices' hardware. The workflow of *B-AUT* contains three parts. Before authentication, we leverage a fuzzy fingerprint and EPC to jointly cluster the raw data collected from tags' backscatter signals into groups, and thus address the first challenge. During authentication, we can extract the fine-grained fingerprints based on our designed algorithms, validate their genuineness and obtain the invalid clusters. After authentication, to match these invalid fingerprints to corresponding counterfeit tags, we exploit coarse-grained tag localization methods to narrow the search range for finding out dubious tags and conduct small-scale re-validation to eventually pinpoint counterfeit tags in physical space, thereby overcoming the second challenge. Our contributions are summarized as follows:

- **(Parallelism)** To the best of our knowledge, it is the first work to present a Gen2-compatible universal architecture for batch tags' simultaneous authentication and precisely pinpointing the counterfeit tags in physical space. Moreover, we prove the theoretical upper bound of counterfeit tags' number with same EPC during simultaneous authentication. Note that, the only batch authentication methods [23]–[25] require modifications on Gen2 protocols and thus can not deploy on commodity tags. Actually, they only conduct simulations rather than real-world experiments and can not render the pinpointing function as well. Up to now, very few works are able to achieve batch tags authentication indeed.
- **(Universality)** *B-AUT* is applicable to almost all existing hardware fingerprints extracted by diverse RF devices without any hardware or firmware modifications. Even when only one commercial RFID reader with a single antenna is utilized, *B-AUT* can still work.
- **(Effectiveness)** We implement a prototype of *B-AUT* and evaluate it in extreme cases (*i.e.*, low-capability devices and concise methods). Experiment results verify that *B-AUT* is effective to achieve nearly the same accuracy of batch authentication as that of separate authentication, and reduce the time overhead by 43.25%. Moreover, the pinpointing accuracy of *B-AUT* can also reach 92.8%.

[2]For a universal architecture, we should consider not only RF devices with strong capability (like SDR), but also the most ordinary device [20], [21], *i.e.*, one commercial reader with a single antenna.

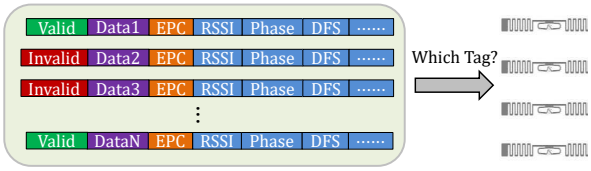

Fig. 3. The challenge of pinpointing tags with invalid fingerprints

The rest of the paper is organized as follows. The past works related to tag authentication are discussed in Section II. The architecture design and methodology are introduced in Section III. The experimental implementation and performance evaluation of *B-AUT* are detailed in Section IV. Finally, the conclusion is summarized in Section V.

II. Related Work

Tag authentication based on hardware fingerprints: in recent works, manufacturing imperfection-induced hardware diversity inside backscatter signal features are leveraged as fingerprints, *e.g.*, time interval error, average baseband power and spectral features [8], covariance-based pulse and power spectrum density [16], phase noises [14], persistence time [17], and differential noises in the frequency domain [15]. Different fingerprints have their own pros and cons respectively, *e.g.*, persistence time is resistant to multipath reflections but suffers from high latency; differential noises can eliminate the impacts of reader hardware but incurs more tags deployment. Meanwhile, extracting different fingerprints needs diverse RF devices, *e.g.*, SDR and spectral analyzers [14]–[18]. In different scenarios, these devices are uncertain to be all available and which fingerprint to be used also depends on the practical requirements. Accordingly, a universal architecture that applies to existing fingerprints for building adaptive RFID authentication systems is necessary to explore.

Batch authentication: though those works propose numerous fingerprints, they can only authenticate tags one by one and fail simultaneous authentication of multiple tags, probably due to our mentioned two challenges. Few works achieve this, and the only batch authentication approaches [23]–[25] are not compatible with Gen2 standard and fail to conduct real-world experiments, which is hard to verify their practical effects.

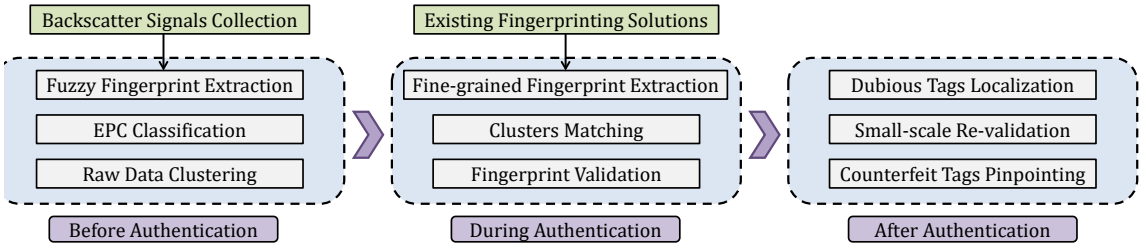

Fig. 4. Architecture overview of *B-AUT*

As a result, high time overhead and human efforts would be incurred if existing methods employed. Moreover, they can only determine whether the collected signal data are valid, but fail to pinpoint the corresponding counterfeit ones from batch tags and destroy them, which is also very critical since the purpose of tag authentication is to find out the forged items and handle them. In summary, a universal architecture for batch authentication is a vital but still unsolved issue.

III. Architecture Design

As shown in Fig. 4, *B-AUT* contains three modules and the technical details are introduced in the following subsections. Note that to ensure the universality, the leveraged fingerprints and methodology here should be applicable to signal features commercial readers can collect. The purpose of our architecture *B-AUT* is to render a framework and more well-refined inner methods are also encouraged based on our design.

A. Before Authentication

The purpose before authentication is to cluster all sets of raw data into groups and address the first challenge.

Each set of raw data can generate its own fuzzy fingerprint based on received signal strength indication (RSSI), phase shift and Doppler frequency shift (DFS). Here the fuzzy fingerprint means the both hardware and environment-related fingerprint that is only utilized to determine which sets of data belong to the same tag[3], but not exploited to validate the genuineness. Specifically, we can obtain the interval of each set's phase $[\phi - \Delta\phi, \phi + \Delta\phi]$ in terms of DFS as follows.

$$\Delta\phi_i = \left| F_m^i \cdot 4\pi\Delta T \right|, \ \forall i \in \mathcal{N} \tag{1}$$

where F_m^i denotes the collected DFS of i-th set and ΔT denotes the time duration of a packet determined by backscatter link frequency. ϕ_i is the collected phase shift of i-th set and $\Delta\phi_i$ determines the interval of ϕ_i. $\mathcal{N} = \{1, 2, ..., N\}$ where N is the total number of sets.

Due to that signal features data from the same tag should approach to each other, *e.g.*, $P_i \approx P_j$ if i-th and j-th sets of data belong to the same tag where P_i denotes the collected RSSI of i-th set, we can leverage $\langle P_i, \phi_i, \Delta\phi_i \rangle$ as fuzzy fingerprint of i-th set, denoted by ψ_i.

Then, we define the following rules for clustering all sets into groups, by jointly using EPC and fuzzy fingerprint.

[3]For simplicity, we consider the scenarios of stationary tags (*e.g.*, warehouse inventory), where tags' locations would not change in a short time.

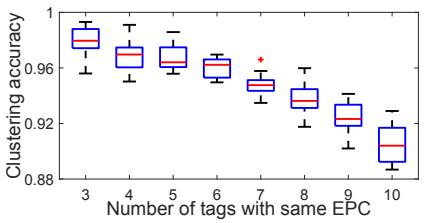

Fig. 5. The clustering accuracy vs. number of tags with same EPC. The accuracy reaches 100% when tag's number is one or two. Note that the accuracy is independent of tags' total quantities.

First step: we initially regard each set of data as one cluster.

Second step: we calculate the maximum Euclidean distance between each two clusters' data if their EPC are same, and regard the distance infinity between two clusters with different EPC. That is,

$$dist(c_p, c_q) = \max_{i \in c_p, j \in c_q} [\|\psi_i - \psi_j\|, +\infty]^+ \tag{2}$$

where c_p and c_q denote p-th and q-th clusters respectively, and (i, j) are sets in two clusters. $[x, +\infty]^+$ equals x when two clusters' EPC are same, otherwise it equals infinity since each two clusters with different EPC cannot belong to the same tag.

To calculate $\|\psi_i - \psi_j\|$, we define a coefficient ω to measure the similarity of phases as

$$\omega = (\phi_i - \phi_j)^2 \cdot e^{\frac{(\phi_j - \phi_i)^2}{2(\tilde{\sigma} + \Delta\phi_i/\beta)^2} + \frac{(\phi_i - \phi_j)^2}{2(\tilde{\sigma} + \Delta\phi_j/\beta)^2}}, \tag{3}$$

and normalize RSSI difference to jointly obtain the distance. Here ϕ is regarded as a Gaussian distribution and β is an empirical positive integer where the probability inside $[\phi_i - \Delta\phi_i, \phi_i + \Delta\phi_i]$ approaches one (*e.g.*, the probability reaches 0.997 when $\beta = 3$). $\tilde{\sigma}$ is a small term to avoid $\Delta\phi = 0$. For the cases with wrapped phases (*i.e.*, $\phi \approx 0$ or 2π), we consider to translate two phases into a comparable state using $\phi \pm 2\pi$, and the recomputed distance with higher similarity is regard as $\|\psi_i - \psi_j\|$.

Third step: we utilize bottom-up hierarchical clustering method [26] to iteratively update the clusters and their mutual distances by repeating the second step. The termination criterion is determined by an empirical threshold δ as follows.

$$dist(c_p, c_q) \geq \delta, \forall p, q \in \{1, 2, ..., L\}, p \neq q \tag{4}$$

where L denotes the number of clusters in current iteration.

In this way, we can obtain M clusters consisting of all sets and each cluster is corresponded to one specific tag. The whole algorithm is exhibited in Algorithm 1. Here we conduct

Algorithm 1: Raw Data Clustering Algorithm

Input: EPC and fuzzy fingerprint $\langle P_i, \phi_i, \Delta\phi_i \rangle$ of i-th set ($i \in \mathcal{N}$)

Output: M clusters

Initialize all sets of data as N clusters;

repeat

  Calculate and update $dist(c_p, c_q)$ for each pair of clusters (c_p, c_q) by using (2) and (3);

  Unwrap ϕ and recompute $dist(c_p, c_q)$ for each (c_p, c_q);

  Find the clusters with minimum $dist(c_p, c_q)$ and merge them into one cluster;

until *there exist no distances less than* δ;

an experiment for verification using one ImpinJ R420 reader [27] with a single Laird S9028PCL antenna and ten Alien AZ-9662 tags [28], and the results of clustering accuracy are illustrated in Fig. 5. We can find that our algorithm maintains a fine accuracy over the increasing number of tags with same EPC. We believe more antennas used could help improve the resolution ratios and further the clustering accuracy.

B. During Authentication

The purpose during authentication is to extract fine-grained hardware fingerprints of tags (*i.e.*, clusters), validate them and obtain the invalid clusters.

To show the universality, here we leverage the phase noise ϕ_T proposed in TagPrint [14] as fingerprint, which can be extracted by commercial devices. In practice, ϕ_T is a part of average unwrapped phase shift $\hat{\phi}$ in each cluster [12], *i.e.*,

$$\hat{\phi}_k = \phi_{T_k} + \phi_R + 2\pi \times \frac{2d_k}{\lambda} \mod 2\pi, \ \forall k \in \mathcal{M} \quad (5)$$

where ϕ_{T_k} denotes the phase noise of k-th tag and ϕ_R denotes the noise induced by reader's circuits. d_k is the distance between the k-th tag and reader antenna, and λ is the RFID signals' wavelength. Let $\mathcal{M} = \{1, 2, ..., M\}$.

To extract ϕ_T and alleviate the impact of d, we consider to move the reader antenna for collection twice and exploit the differential RSSI (like Tagtag [29]). Due to the relationship of average differential RSSI $\Delta\hat{P}$ and differential distance Δd:

$$\frac{d_k + \Delta d_k}{d_k} = 10^{\frac{-\Delta\hat{P}_k}{40}}, \ \forall k \in \mathcal{M} \quad (6)$$

where Δd should better be lower than $\lambda/2$, and the relationship of differential phase shift $\Delta\hat{\phi}$ and Δd:

$$\frac{d_k + \Delta d_k}{d_k} = \frac{\hat{\phi}_k + \Delta\hat{\phi}_k - \phi_{T_k} - \phi_R + \vartheta + \Delta\vartheta}{\hat{\phi}_k - \phi_{T_k} - \phi_R + \vartheta}, \forall k \in \mathcal{M} \quad (7)$$

where $\Delta\vartheta = 0$ or 2π to avoid wrapped phases' impact, we can obtain ϕ_{T_k} $(k \in \mathcal{M})$ by the following equation

$$\phi_{T_k} = \frac{(10^{\frac{-\Delta\hat{P}_k}{40}} - 1)(\hat{\phi}_k + \vartheta) - \Delta\hat{\phi}_k - \Delta\vartheta}{(10^{\frac{-\Delta\hat{P}_k}{40}} - 1)} - \phi_R \quad (8)$$

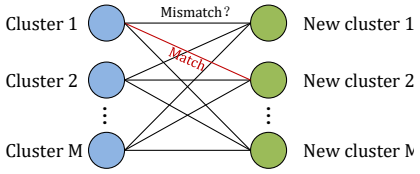

Fig. 6. Clusters matching after reader antenna movement

where ϕ_R is only a stable constant for all tags and we can implicitly use $\phi_{T_k} + \phi_R$ as the fingerprint. The value of ϑ and $\Delta\vartheta$ can be determined by the calculated result since the range of $\phi_{T_k} + \phi_R$ is $[0, 2\pi]$.

However, there remains a big problem to solve: how can we find the same tag's cluster after reader antenna movement, *i.e.*, the clusters matching as shown in Fig. 6. Here we propose a matching algorithm as follows, based on two properties: only two clusters with same EPC would belong to the same tag; at most one pair of clusters could have the same hardware fingerprint as the registered one.

First step: for each cluster k and any new cluster u with same EPC, we define $\eta_{k,u} = 1$ to represent the possibility of this pair; otherwise, we set $\eta_{k,u} = 0$.

Second step: for each (k, u) with $\eta_{k,u} = 1$, we can calculate the hardware fingerprint $\phi_T(k, u)$ of this pair via (8).

Third step: for each (k, u), we define $\hat{\eta}_{k,u}$ which determines whether k-th and u-th clusters belong to the same tag or not. If $\eta_{k,u} = 0$, we set $\hat{\eta}_{k,u} = 0$; for any k, if only one u satisfies $\eta_{k,u} = 1$, we set $\hat{\eta}_{k,u} = 1$.

Fourth step: for each EPC α with multiple possible pairs of clusters, we choose the pair with minimal gap between obtained $\phi_T(k, u)$ and the corresponding registered one $\tilde{\phi}_T(\alpha)$ as follows. In this way, we can iteratively obtain $\hat{\eta}$.

$$[k^*, u^*] = \underset{(k,u)\in\mathcal{H}(\alpha)}{\arg\min} \left| \phi_T(k, u) - \tilde{\phi}_T(\alpha) \right| \quad (9)$$

where $\hat{\eta} = \{\hat{\eta}_{k,u} | k, u \in \mathcal{M}\}$ and $\mathcal{H}(\alpha)$ is the set of cluster pairs with same EPC α. In each iteration, the updating rules for $\hat{\eta}$ are: utilizing (9) to find out the optimal pair (k^*, u^*), updating the $\hat{\eta}_{k^*,u^*} = 1$ and then $\hat{\eta}$ according to $\sum_k \hat{\eta}_{k,u} = \sum_u \hat{\eta}_{k,u} = 1$, and fixing it as a constraint. After all EPC are scanned in descending order of similarity in (9), the update is terminated. For the rest pairs in $\mathcal{H}$, we match them based on the continuity of signal features under slight antenna movement. In this way, we could at least guarantee the matching correctness of legitimate tags and the illegitimate ones originally should not pass validation even with small matching errors.

Fig. 7. An example of fingerprint validation results

Algorithm 2: Clusters Matching Algorithm

Input: $\hat{\phi}_k$,$\Delta\hat{\phi}_k$ and $\Delta\hat{P}_k$ $(k \in \mathcal{M})$
Output: $\hat{\eta}$ and ϕ_{T_k} $(k \in \mathcal{M})$
Initialize $\eta_{k,u}$ and $\hat{\eta}_{k,u}$ $(k, u \in \mathcal{M})$;
for $k \leq M$ *and* $u \leq M$ **do**
  if *the EPC of* k*-th and* u*-th cluster are same* **then**
    $\eta_{k,u} \leftarrow 1$;
    Calculate $\phi_T(k, u)$ by using (8);
  else
    $\eta_{k,u} \leftarrow 0; \hat{\eta}_{k,u} \leftarrow 0$;
  end
end
for $k \leq M$ **do**
  if *only* u *satisfies* $\eta_{k,u} = 1$ **then**
    $\hat{\eta}_{k,u} \leftarrow 1$;
  end
end
repeat
  Solve (9) and obtain (k^*, u^*) for each EPC;
  Update $\hat{\eta}$ and fix $\hat{\eta}_{k^*,u^*}$;
until *all EPC are scanned*;
Match the rest clusters based on the continuity;
Calculate ϕ_{T_k} $(k \in \mathcal{M})$ based on $\hat{\eta}$.

By these steps, we can eventually know the matching results $\hat{\eta}$ and obtain each cluster's fingerprint ϕ_T. The whole algorithm is given in Algorithm 2. Note that we can also calculate the distribution of ϕ_T, by using all data of each cluster instead of average value. After fine-grained fingerprints extraction, we validate them by jointly identifying EPC and calculating the similarity with registered ones. If there exists more than one cluster passing validation and owning the same EPC, we treat the one with highest similarity as valid cluster. Fig. 7 shows an example of six tags' fingerprint validation results. In this way, we can select U invalid clusters (*i.e.*, U counterfeit tags) from M clusters (*i.e.*, M tags in total).

C. After Authentication

The purpose after authentication is to match U invalid fingerprints to corresponding counterfeit tags because all tags' backscatter signals are collected together and we cannot directly distinguish them in physical space.

To this end, we exploit coarse-grained tag localization methods to narrow the search range to find dubious tags and further conduct small-scale re-validation to eventually pinpoint counterfeit tags in physical space due to the localization error. Specifically, we can utilize collected differential phase shifts before and after reader antenna movement to construct a hyperbola [31] and then RSSI to determine the rough location [32] on this hyperbola, since the antenna is directional and the 2D plane of tags is fixed in the general scenario. Then, we set an empirical threshold ε. The tags with Euclidean distances to localized points shorter than ε are regarded as dubious tags. Let $\mathcal{U} = \{1, 2, ..., U\}$, Q_k denote the number of dubious tags within the localized range of the k-th invalid cluster $(k \in \mathcal{U})$. Due to the localization error, especially when with low-capability RF devices and concise localization method, it is necessary to conduct small-scale re-validation as follows.

Algorithm 3: Counterfeit Tags Pinpointing Algorithm

Input: k-th cluster's fingerprints $(k \in \mathcal{U})$
Output: U counterfeit tags
Initialize υ as an empirical parameter and optimize it;
for $k \leq U$ **do**
  Re-validate each υ dubious tags (a team);
  repeat
    Find the target team;
    Narrow the search region;
    Re-validate each $\upsilon/2$ tags like step 3;
  until *there exists only one tag*;
end
The residual U tags are regarded as counterfeit ones.

First step: for k-th localized range, we consider to decrease the transmission power of RFID reader antenna (theoretically reading υ tags at a time and these tags forming a team), move it along horizontal and vertical $\pm\varepsilon$ displacement with a proper step (forming γ teams with all Q_k tags included), and re-validate each team's dubious tags, by Select-Query commands to filter EPC. If no tags matched, we can adjust the matching results of invalid clusters in Algorithm 2.

Second step: next we search the target team whose region contains the dubious tag with same EPC and is farthest to the position of valid tag carrying this EPC via the same localization method above, from all γ teams. In this way, the number of dubious tags is reduced from Q_k to υ.

Third step: we can further decrease the antenna's transmission power to reduce υ by nearly a half and conduct the next-round re-validation in the target team's region. We repeat the above steps until there exists only one tag in the target team, and the residual dubious tag in the end is regarded as k-th counterfeit tag.

As summarized in Algorithm 3, we can finally pinpoint all U counterfeit tags in physical space as shown in Fig. 8, thereby addressing the second challenge. Moreover, we notice that larger υ would incur more rounds to find out the residual tag, whereas smaller υ would increase the number of locations for signal collection. Thus, we try to reduce the time overhead

Fig. 8. An example of pinpointing counterfeit tags

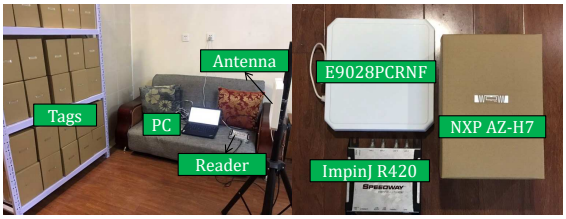

Fig. 9. Experiment Setup of *B-AUT*

of Algorithm 3 by trading off υ as follows.

$$\upsilon^* = \arg\min_{\upsilon \in \mathbb{N}_+} \sum\nolimits_{\zeta} \gamma\left(\frac{\upsilon}{2^{\zeta-1}}\right)\left(\tau_0 + \tau\left(\frac{\upsilon}{2^{\zeta-1}}\right)\right) \tag{10}$$

where $\tau(\upsilon)$ denotes the time overhead of re-validation on υ tags and $\gamma(\upsilon)$ denotes the required locations' quantities to collect all tags' signals during antenna moving under υ. Both the functions $\tau(\upsilon)$ and $\gamma(\upsilon)$ could be obtained through empirical studies. τ_0 denotes the basic time of signal collection before re-validation starts. We can solve (10) by calculating its derivative and obtain the optimized υ since there exist no constraints. In practice, we can adjust the transmission power to reset the optimal value of υ.

D. Practical Issues

We should emphasize that *B-AUT* does not focus on proposing new hardware fingerprints or authentication methods, but building a universal architecture that is compatible with existing fingerprints, addressing two critical challenges with novel approaches and achieving batch tags authentication.

The total number of tags M would not affect the performance of *B-AUT* but the number of tags carrying the same EPC (denoted by M_s) would. Taking our utilized fingerprint (*i.e.*, phase noise) as an example, we can further prove that the theoretical upper bound of M_s during simultaneous authentication is around $\lfloor 2\pi/0.5 \rfloor = 12$ where 0.5 is the approximate resolution ratio of this hardware fingerprint. With a distribution of phase noise, the upper bound can be promoted by 2∼3×.

In conclusion, *B-AUT* renders a formalized framework with advantages of parallelism, universality and effectiveness on batch tags authentication.

IV. Implementation and Evaluation

To verify the performance of *B-AUT*, we implement a prototype of *B-AUT* using one ImpinJ Speedway R420 reader which is connected to our ThinkPad PC as the handler through Ethernet based on low level reader protocol (LLRP) [33] with a single E9028PCRNF circular polarized antenna whose gain is 8dBi, and 100 NXP AZ-H7/Alien AZ-9662/ImpinJ H47 passive tags [27], [28], [34]. All RF devices operate on the UHF band of 920.625MHz∼924.375MHz. The *B-AUT* software including our algorithms is implemented using Java (OctaneSDKJava-1.20.2.240 [35]) and Matlab. We conduct real-world experiments and evaluate the performance of items inventory during one week in a private warehouse, as shown in Fig. 9.

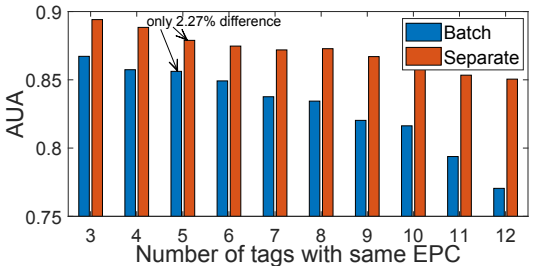

Fig. 10. AUA vs. number of tags with same EPC

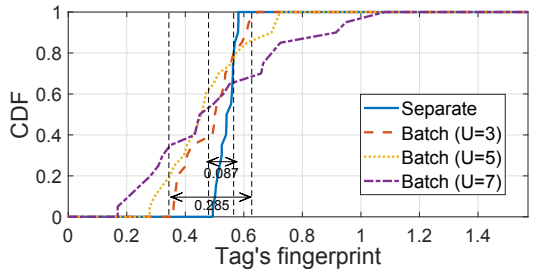

Fig. 11. CDF curves of tag's fingerprint in separate/batch authentication

Our experiments mainly contain two parts. One is to measure the parallelism and effectiveness of *B-AUT* under different numbers and types of devices. To verify the universality, we only need to evaluate it in aforementioned extreme case because devices with strong capability (like SDR) can also realize the functions of weakest devices (*i.e.*, commercial reader with a single antenna) and further the extraction of same fingerprint. The other is to evaluate *B-AUT* under different settings (*e.g.*, thresholds, RF channels). The evaluation metrics used are average authentication accuracy (AUA) that means the proportion of successful authentication (*i.e.*, legitimate tags passing and counterfeit tags failing), time overhead (TIO) that means the total duration of *B-AUT*'s whole process and pinpointing accuracy (PIA) that means the proportion of successfully matching invalid clusters to tags in physical space.

A. Performance of batch authentication

First, we change the total number of tags ($\hat{M}$) from 10 to 50 and also the number of tags with same EPC ($\hat{U}$) from 3 to 9, where $\hat{U} = x \times y$ means x sets with y tags carrying same EPC

TABLE I
Performance evaluation under different number of tags

$\hat{M}$	$\hat{U}$	AUA	PIA	TIO
10	1×3	**83.3**%	**92.8**%	15.2s
10	2×3	77.2%	88.1%	17.4s
10	3×3	67.8%	84.9%	20.3s
25	1×3	**82.4**%	**91.2**%	26.5s
25	2×3	74.5%	85.8%	27.2s
25	3×3	66.2%	84.1%	30.7s
50	1×3	**80.8**%	**90.3**%	48.5s
50	2×3	74.3%	87.5%	50.2s
50	3×3	65.1%	83.5%	54.5s

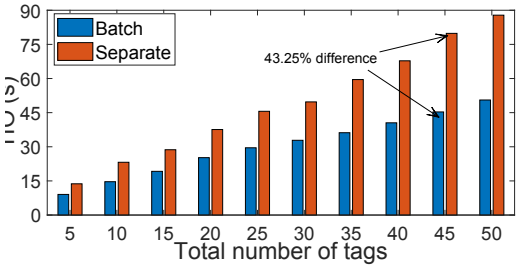

Fig. 12. TIO vs. total number of tags

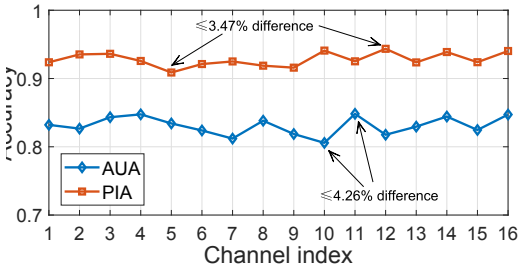

Fig. 13. AUA and PIA vs. used RF channel

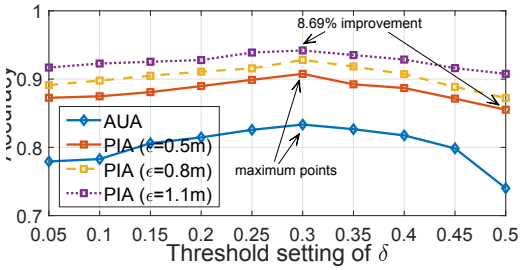

Fig. 14. AUA and PIA vs. threshold settings of δ and ε

in each set. From the results in Table I, we can find that both AUA and PIA nearly do not change (less than 2.5%) with the increasing $\hat{M}$ when $\hat{U}$ is fixed, while AUA drops sharply when $\hat{U}$ raises. This conforms to our corollary that the limitation to *B-AUT*'s performance is not $\hat{M}$ but $\hat{U}$ because tags with different EPC must be classified into distinct clusters and matched correctly, and the error cases are incurred by tags with same EPC. This also verifies the effectiveness of our proposed clustering and matching algorithms and the high parallelism to achieve batch tags authentication. The high PIA of up to 92.8% also demonstrates the effectiveness of our small-scale re-validation algorithm. Note that PIA is independent of AUA that is determined by past fingerprints and it reflects purely the effects of pinpointing accuracy. In addition, though AUA decreases with larger $\hat{U}$, we believe more antennas or devices with stronger capability used would improve AUA and PIA a lot. Meanwhile, in terms of TIO, we can find that the effect of $\hat{M}$ is stronger than that of $\hat{U}$ though TIO is inevitable to be prolonged with both increasing $\hat{M}$ and $\hat{U}$. This is probably because a larger total number of tags not only incurs longer latency of signal collection, but also increases the overhead in our proposed three algorithms. Nevertheless, the growth of TIO shows an approximately linear tendency with increasing $\hat{M}$ and thus is acceptable for batch authentication.

Second, we evaluate *B-AUT* in batch authentication and separate authentication which means authenticating tags one by one, respectively in the same environment. As shown in Fig. 10, compared to the AUA of separate authentication, *B-AUT* can maintain nearly the same AUA with only 2.27% decreases. Even when $\hat{U}$ approaches the given theoretical upper bound 12, the difference is also lower than 8%. Fig. 11 where the CDF curves of tag's fingerprint are similar to each other (with a difference less than 0.2) also demonstrates that *B-AUT* would not limit the original performance of existing fingerprints. Exploiting a more well-refined fingerprint than phase noise can probably promote the upper bound of $\hat{U}$ and further AUA. In summary, these observations all reveal *B-AUT*'s effectiveness. In another aspect, *B-AUT* can reduce the TIO by up to 43.25% as compared to that of separate authentication (see Fig. 12). Besides, it practically can save human efforts and reduce more time cost in real-world applications.

Third, we adjust the tag models and conduct the same experiments. Table II demonstrates that *B-AUT* can work with different types of tags, holding high AUA, PIA and low TIO. The maximum differences of AUA and PIA are only 5.6% and 1.9%, generally due to that the hardware diversity of Alien AZ-9662 tags is lowest and ImpinJ H47 tags are more robust to environmental changes. The maximum difference of TIO is 3.2s and it is reasonable because ImpinJ H47 tags have double dipole antennas, thereby shorten the signal collection duration. In conclusion, *B-AUT* can achieve high authentication performance regardless of tag models.

B. Performance under different settings

Here we consider to measure the effect of used RF channel by hopping it continuously. From Fig. 13, we can find both AUA and PIA remains stable across channels, with maximum differences of 3.47% and 4.26% respectively. The variances are probably induced by environmental multipaths since the effect of multipath signals on different channels shows diversity [36]. In practical use, we can simply select the optimal channel with minimum signal features varieties for communication.

Next, we change the threshold values of δ and ε to evaluate their effects on AUA and PIA. As shown in Fig. 14, on one hand, both bigger and smaller δ would lead to lower AUA and PIA (down to 74.0% and 85.5% respectively) because bigger δ corresponded to more coarse-grained clustering increases the risk that different tags' data are clustered into the same group and jeopardizes extracted fingerprints, while smaller

TABLE II
PERFORMANCE EVALUATION UNDER DIFFERENT TAG MODELS

Provider	Tag model	AUA	PIA	TIO
NXP	AZ-H7	83.3%	92.8%	15.2s
Alien	AZ-9662	80.2%	92.4%	14.8s
ImpinJ	H47	85.8%	94.3%	12.0s

δ may cause the wrong case that data from the same tag are not clustered together and raise both the false reject rate and the possibility of falsely pinpointing. On the other hand, bigger ε corresponded to larger searching space of dubious tags is preferred so that the PIA can be improved by 8.69%, but inevitably TIO would be prolonged likewise. Thus, the setting value of ε should be traded off according to practical requirements.

V. Conclusion

In this paper, we present a universal architecture, namely *B-AUT* for batch RFID tags authentication based on a series of our proposed algorithms, which is fully compatible with Gen2 specification and existing hardware fingerprints. Experiment results show that *B-AUT* can maintain high accuracy in simultaneous authentication, reduce the time overhead as compared to previous separate authentication, and also effectively pinpoint the counterfeit tags in physical space.

Acknowledgment

This work is supported partially by the National Key Research and Development Program of China (Grant No.2018YFB0803403), the National Natural Science Foundation of China (Grant No.61902212), and the Beijing Institute of Technology Research Fund Program for Young Scholars.

References

[1] L. Shangguan, Z. Yang, A. X. Liu, Z. Zhou, and Y. Liu, "Relative localization of rfid tags using spatial-temporal phase profiling," in *Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2015, pp. 251–263.

[2] Z. An, Q. Lin, X. Zhao, L. Yang, D. Zheng, G. Wu, and S. Chang, "One tag, two codes: identifying optical barcodes with nfc," in *Proceedings of ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2021, pp. 108–120.

[3] Y. Zhu, C. Duan, and X. Ding, "Accurate and fast detection of tag antenna damage for rfid sensing," in *Proceedings of ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI)*, 2021, pp. 269–270.

[4] T. Shi, Z. Cai, J. Li, and H. Gao, "Joint deployment strategy of battery-free sensor networks with coverage guarantee," *ACM Transactions on Sensor Networks (TOSN)*, vol. 17, no. 4, pp. 1–29, 2021.

[5] S. Li, M. Arslan, A. Khojastepour, S. V. Krishnamurthy, and S. Rangarajan, "Deeptrack: Grouping rfid tags based on spatio-temporal proximity in retail spaces," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2020, pp. 1271–1280.

[6] C. Duan, J. Liu, X. Ding, Z. Li, and Y. Liu, "Full-dimension relative positioning for rfid-enabled self-checkout services," *Proceedings of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 5, no. 1, pp. 1–23, 2021.

[7] L. Shangguan, Z. Zhou, X. Zheng, L. Yang, Y. Liu, and J. Han, "Shopminer: Mining customer shopping behavior in physical clothing stores with cots rfid devices," in *Proceedings of ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2015, pp. 113–125.

[8] D. Zanetti, B. Danev, and S. Mapkun, "Physical-layer identification of uhf rfid tags," in *Proceedings of ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2010, pp. 353–364.

[9] A. Juels, "Rfid security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 24, no. 2, pp. 381–394, 2006.

[10] G. Wang, H. Cai, C. Qian, J. Han, X. Li, H. Ding, and J. Zhao, "Towards replay-resilient rfid authentication," in *Proceedings of ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2018, pp. 385–399.

[11] 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 *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2020, pp. 2194–2203.

[12] D. M. Dobkin, *The RF in RFID: UHF RFID in practice*. Newnes, 2012.

[13] V. Chawla and D. S. Ha, "An overview of passive rfid," *IEEE Communications Magazine*, vol. 45, no. 9, pp. 11–17, 2007.

[14] 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 *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2015, pp. 1966–1974.

[15] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive rfid," *Proceedings of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 2, no. 4, pp. 1–21, 2018.

[16] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao, "Geneprint: Generic and accurate physical-layer identification for uhf rfid tags," *IEEE/ACM Transactions on Networking (ToN)*, vol. 24, no. 2, pp. 846–858, 2015.

[17] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: Robust energy-related fingerprinting for passive rfid tags," in *Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2020, pp. 1101–1113.

[18] M. Piva, G. Maselli, and F. Restuccia, "The tags are alright: Robust large-scale rfid clone detection through federated data-augmented radio fingerprinting," *arXiv preprint arXiv:2105.03671*, 2021.

[19] E. Global, "Specification for rfid air interface epc radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz-960 mhz," Technical report, GS1, Tech. Rep., 2008.

[20] H. Jin, J. Wang, Z. Yang, S. Kumar, and J. Hong, "Wish: Towards a wireless shape-aware world using passive rfids," in *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2018, pp. 428–441.

[21] J. Zhao, J. Li, D. Li, and H. Yang, "Optimal data transmission in backscatter communication for passive sensing systems," *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 647–658, 2020.

[22] L. Yang, J. Han, Y. Qi, C. Wang, Y. Liu, Y. Cheng, and X. Zhong, "Revisting tag collision problem in rfid systems," in *Proceedings of IEEE International Conference on Parallel Processing (ICPP)*, 2010, pp. 178–187.

[23] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification-free batch authentication for rfid tags," in *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, 2010, pp. 154–163.

[24] W. Gong, K. Liu, X. Miao, Q. Ma, Z. Yang, and Y. Liu, "Informative counting: Fine-grained batch authentication for large-scale rfid systems," in *Proceedings of ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2013, pp. 21–30.

[25] Q. Lin, L. Yang, and Y. Guo, "Proactive batch authentication: Fishing counterfeit rfid tags in muddy waters," *IEEE Internet of Things Journal (IoTJ)*, vol. 6, no. 1, pp. 568–579, 2018.

[26] F. Murtagh, "A survey of recent advances in hierarchical clustering algorithms," *The Computer Journal*, vol. 26, no. 4, pp. 354–359, 1983.

[27] "Impinj inc," http://www.impinj.com.

[28] "Alien technology," http://www.alientechnology.com.

[29] B. Xie, J. Xiong, X. Chen, E. Chai, L. Li, Z. Tang, and D. Fang, "Tagtag: material sensing with commodity rfid," in *Proceedings of ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2019, pp. 338–350.

[30] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[31] T. Liu, Y. Liu, L. Yang, Y. Guo, and C. Wang, "Backpos: High accuracy backscatter positioning system," *IEEE Transactions on Mobile Computing (TMC)*, vol. 15, no. 3, pp. 586–598, 2015.

[32] Y. Liu, Z. Yang, X. Wang, and L. Jian, "Location, localization, and localizability," *Journal of Computer Science and Technology (JCST)*, vol. 25, no. 2, pp. 274–297, 2010.

[33] E. EPCglobal, "Low level reader protocol (llrp)," 2010.

[34] "Nxp," https://www.nxp.com.

[35] "Octanesdkjava," http://platform.impinj.com/site/docs/octane/_SDK.

[36] G. Wang, C. Qian, K. Cui, X. Shi, H. Ding, W. Xi, J. Zhao, and J. Han, "A universal method to combat multipaths for rfid sensing," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2020, pp. 277–286.