Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6718689, 13 pages
https://doi.org/10.1155/2022/6718689

Research Article

An Effective and Robust Method for Unauthorized Reader Detection Based on Tag's Energy

Ziwen Cao,[1,2] **Jinxing Xie**,[1,2] **Siye Wang**,[1,2] **Yanfang Zhang**,[1] **Yue Cui**,[1,2] **Shang Jiang**,[1,2] **and Biao Jin**[3]

[1]*Institute of Information Engineering, Chinese Academy of Sciences, China*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, China*
[3]*National Security Science and Technology Evaluation Centre, Beijing, China*

Correspondence should be addressed to Siye Wang; wangsiye@iie.ac.cn

Received 23 January 2022; Revised 15 July 2022; Accepted 27 August 2022; Published 7 October 2022

Academic Editor: Yinghui Ye

With the rapid development of the Internet of Things, ultra-high frequency (UHF) passive radio frequency identification (RFID) technology plays a vital role in various fields. UHF RFID faces unauthorized access attacks due to its long identification distance. Unauthorized readers can hide within a certain distance and use standard commands to read or modify tags. However, existing methods require additional equipment or are susceptible to environmental influences. In this paper, we make a novel attempt to counterattack unauthorized access. We propose a new method for Unauthorized Reader Detection based on Tag's Energy, called URDTE, to detect unauthorized readers by observing the energy of the tag. The competitive advantage of URDTE is that it is fully compatible with the RFID standard EPCglobal Gen 2, which makes it more applicable and scalable in practice. Besides, it takes the electrical energy stored in a tag's resistor-capacitor (RC) circuit as the detection principle, which is robust to environmental changes such as tag position, communication distance, and transmit power. We implement URDTE using commercial off-the-shelf (COTS) RFID devices without requiring firmware or hardware modifications. Extensive experiments show that URDTE can detect unauthorized readers with an accuracy of up to 99%.

1. Introduction

Radio frequency identification (RFID) is a noncontact automatic identification technology widely used in commercial automation, industrial automation, transportation, and many other fields, such as intelligent traffic control systems, access control systems, and warehouse management [1]. This technology uses the backscattering characteristics of radio frequency signals to achieve automatic identification [2] and mainly relies on two devices: tags (which can emit radio signals encoding identifying information) and readers (which detect the signals emitted by tags). RFID technology realizes item identification, inventory, and positioning by sticking tags on different items and placing the reader in the appropriate position. RFID tags are divided into active tags and passive tags. Active tags are expensive and only used in a few scenarios. Passive tags are widely used in all walks of life because they do not need a built-in power supply and have the advantages of low price, small volume, and long service life.

Due to the simple internal structure of the passive electronic tag chip and the weak computing power, the security protection ability of the RFID tag is poor. Many intrusion attacks against RFID systems are conducted against RFID tags. The most common attack is the unauthorized reading attack. The root cause of this problem is that there is no stipulation for tag-reader authentication in the existing RFID communication specification (i.e., EPCglobal Class 1 Generation 2 protocol [3, 4], referred to as EPCglobal Gen 2 in the following). In other words, RFID tags do not have the ability to authenticate the reader's identity, causing the tag to respond to any reader that accesses itself, which will lead to the following two risks. On the one hand, RFID tags send data in clear text. When a malicious reader compatible with

this protocol get close to the tag, the plaintext information of the tag can be obtained, resulting in the risk of privacy leakage. On the other hand, attackers use malicious readers to impersonate legal RFID readers and create tags with the same tag code, resulting in the risk of data tampering. As an example, the commercial spy may use the high-power reader to read the commercial rival warehouse's RFID tags to understand the rival situation and its business decision [5].

Meanwhile, security experts put forward protection measures to prevent unauthorized reading attacks, including data encryption, security protocol design, and RFID air interface intrusion detection. The data encryption method encrypts the communication data between the RFID tags and the readers so that the malicious RFID readers cannot parse the data. However, this requires a higher power excitation signal to drive the tag circuit, which dramatically shortens the reading distance of the tag and limits the usage scenarios [6]. Regarding RFID security protocols, scholars have proposed a series of improved security protocols for the security loopholes of existing protocols [7, 8], but these protocols are not universal. In the research of RFID air interface intrusion detection, Razm and Alavi [9] proposed a watchdog reader method to find the abnormal data when the system is working. However, the cost of this method is high due to the need to add additional RFID readers. Ding et al. [10] utilized USRP devices to monitor electromagnetic signals and proposed a fingerprint matching method to detect unauthorized readers. However, this method is not compatible with COTS RFID devices and lacks practicality. In addition, the electromagnetic fingerprint will change continuously with the changes in the environment, resulting in a decrease in detection accuracy.

To solve the unauthorized reading problem, we propose an unauthorized reader detection method based on the tag's power. The core idea is to observe the internal energy of the tag. Passive electronic tags use the electromagnetic signal emitted by the reader antenna to couple with its own antenna to generate electricity. Electrical energy is stored in the tag's internal capacitors to power the tag's internal volatile storage [11]. The energy stored in its internal capacitor lasts for a short period after the tag is accessed. Therefore, when it is detected that the internal circuit of the tag is abnormally charged, it means that the tag has been read without authorization. We designed URDTE (Unauthorized Reader Detection based on Tag's Energy) to detect unauthorized readers based on EPCglobal Gen 2, combined with the scenario of unauthorized reader detection. The specific approach is first to collect the tag's persistence time. Then, we construct models to calculate the persistence time and estimate the best model parameters. Finally, we carry on the real-time unauthorized reader detection. The final experimental results show that URDTE can detect unauthorized reading with a high accuracy rate. The main contributions are as follows:

(1) We explore a new method for malicious reader detection based on the tag's energy, called URDTE. The competitive advantage of URDTE is that it is fully compatible with the RFID standard, which makes it more applicable and scalable in practical applications. Besides, it is based on the power of the tag and is robust to various environmental conditions

(2) We propose a new metric called persistence time to detect malicious readers indirectly. Furthermore, we measure the persistence time by flipping and observing the flag in the tag's volatile memory

(3) We implemented a URDTE prototyping system based on the EPCglobal Gen 2 standard. Extensive experiments show that our method has high detection accuracy on average of 99%

The main structure of this paper is organized as follows: Section 2 describes the related work. Section 3 presents some background knowledge necessary to understand the methodology of this paper, including the EPCglobal Gen 2 protocol, persistence time, and the reading behavior model for unauthorized readers. Section 4 presents the basic principles and the overview of URDTE. Section 5 describes the design of URDTE in detail. Section 6 evaluates the effectiveness of URDTE. Finally, Section 7 concludes the paper.

2. Related Work

Through extensive research, we found that the unauthorized reading problem is mainly solved from two perspectives: defense and detection.

There are two main categories of defensive methods. The first category is to increase the access control protocols to the tag. The reader can only read the tag if it is authenticated by the tag. Burmester and Munilla, Qian et al., and Fan et al. [12–14] propose a lightweight RFID authentication protocol providing powerful authentication capabilities for authentication between tags and readers. Ma and Saxena [15] propose an authentication method based on scene context, where tags only allow access if they have sensed a specific scenario to defend against unauthorized reading. However, whether it is the authentication between the tag and the reader or the authentication with the environmental context, all the methods need to modify the RFID communication protocol or tag construction, which is very difficult for the already large-scale commercial used passive RFID system. Another defense category is to interfere with or intercept the unauthorized reading at the physical layer. Juels et al. [16] proposed a "blocker tag" concept. This "blocker tag" can be a kind of advanced tag or special radio frequency equipment. Such equipment will simulate the behavior of the real tag to interfere with the tag responding to the reader. Although this method can prevent unauthorized readers from accessing the real tag, the "blocker tag" also prevents legal readers from reading the tag and even turn into a DoS attack on the RFID system.

The approach from the detection perspective is to warn when unauthorized reading occurs. There are two main categories of this method. The first type of detection is based on physical layer signal characteristics. Ding et al. and Zhang

et al. [10, 17] utilize USRP devices to monitor electromagnetic signals in the physical space continuously and uses physical layer signal characteristics to detect the presence of unauthorized readings. The second category is the use of application layer data for detection. Sun et al. [18] use the changes in throughput to determine whether there is an unauthorized reading. However, the detection based on physical layer signal characteristics requires additional USRP devices, which leads to system costs increasing. In addition, the use of application layer data for detection is susceptible to interference from various factors, including the environment, which results in poor stability.

In contrast, our method follows the EPCglobal Gen 2 standard and does not require modification of the RFID communication protocol or additional dedicated equipment. As a result, URDTE can run directly on commercial RFID devices, is not easily affected by the environment, and has high detection accuracy and robustness.

3. Preliminaries

To help better understand URDTE, we present some preliminaries to the URDTE approach in this section, mainly including the EPCglobal Gen 2 protocol, the persistence time of RFID tags, and the modeling of unauthorized reading behavior.

3.1. EPCglobal Gen 2 Protocol. The EPCglobal Gen 2 (Gen 2) protocol is a worldwide UHF RFID standard that defines the physical interactions and logical operating procedures between the readers and tags [4]. We highlight the relevant functions involved by URDTE below based on Gen 2.

3.1.1. Session and Inventoried Tag. The EPCglobal Gen 2 standard stipulates that the reader can communicate with the tag through four sessions, respectively *S*0, *S*1, *S*2, and *S* 3. Under each session, there will be *A* or *B* two kinds of inventory flag. The inventory flag is actually a one-bit indicator of the tag's volatile memory. Volatile memory requires power to maintain stored information. Once the power falls below a certain threshold, the stored data is quickly lost and reverts to the default state *A* on each power-up. Tags can use only one session in each round of inventory, and the states under each session do not interfere with each other. Each session needs different power levels to maintain its state, so the persistence time of each inventoried flag is different. Table 1 shows the persistence time of different sessions.

The table shows that in sessions *S*2 and *S*3, the inventory flag will be maintained when the power is applied and maintained for a persistence time greater than 2 seconds after charging has stopped.

3.1.2. Select. Select is a command that is executed first in each round of inventory. This command allows the reader to select the tags to be inventoried. Aside from tag selection, the Select command can also assert or deassert a tags selected (SL) flag, or set a tags inventoried flag to either *A* or *B*. These flags determine whether a tag may respond to the reader or not. There are three core parameters of the Select command, which are as follows:

Table 1: Persistence time under different sessions.

Session	Required persistence time
S0	Tag energized: indefinite
	Tag not energized: none
S1	Tag energized: 500 ms-5 sec
	Tag not energized: 500 ms-5 sec
S2	Tag energized: indefinite
	Tag not energized: >2 sec
S3	Tag energized: indefinite
	Tag not energized: >2 sec

(1) Mask. Mask is used to match with the target tag and is often set to the EPC of the target operation tag.

(2) Target. Target determines whether the Select command operates on SL or four session flags. 0, 1, 2, 3, and 4 represent the operation objects of Session0, Session1, Session2, Session3, and SL, respectively.

(3) Action. The Select command selects the tags according to the rules. It performs different actions on the tags that match and do not match the rules. The specific actions are determined by the parameter Action, which is shown in Table 2.

3.1.3. Query. The Query command is used to initiate a round of inventory. This command is used on the set of tags selected in the previous Select step, or can be used individually. After the reader sends out the Query command, the tag that receives the command will send its information to the reader. After the reader queried the tag using the Query command, it will automatically flip the flag in its current session (from *A* to *B* or *B* to *A*). The Query command mainly consists of three core parameters:

(1) Session. Session determines the session to be used for this round of inventory.

(2) Target. Target determines which status of tags will participate in this round of inventory, where 0 indicates the tags with the session flag being *A* and 1 indicates *B*.

(3) Sel. This parameter is represented by two binary digits and determines which SL state the tag can reply to. 00_2 and 01_2 indicate all matching tags in the previous Select command; 10_2 indicates tags with deasserted SL flag (~ SL); and 11_2 indicates tags with asserted SL flag (SL).

3.2. Persistence Time. When the voltage of the internal energy storage capacitor of the RFID tag reaches above the operating voltage V_0 of the chip circuit, it can supply power to the tag [11]. When the storage capacitor starts to supply power, its supply voltage drops. When it drops below the chip's operating voltage V_0, the storage capacitor loses its power supply capability, the chip will not continue to work, and the data saved in its internal volatile storage area will be lost and reverted to its default value. The period from the decay of a fully charged capacitor to the voltage operating

Table 2: Eight actions of Select.

Action	Tag matching	Tag not-matching
000	Assert SL or inventoried $\longrightarrow A$	Deassert SL or inventoried $\longrightarrow B$
001	Assert SL or inventoried $\longrightarrow A$	Do nothing
010	Do nothing	Deassert SL or inventoried $\longrightarrow B$
011	Negate SL or ($A \longrightarrow B$, $B \longrightarrow A$)	Do nothing
100	Deassert SL or inventoried $\longrightarrow B$	Assert SL or inventoried $\longrightarrow A$
101	Deassert SL or inventoried $\longrightarrow B$	Do nothing
110	Do nothing	Assert SL or inventoried $\longrightarrow A$
111	Do nothing	Negate SL or ($A \longrightarrow B$, $B \longrightarrow A$)

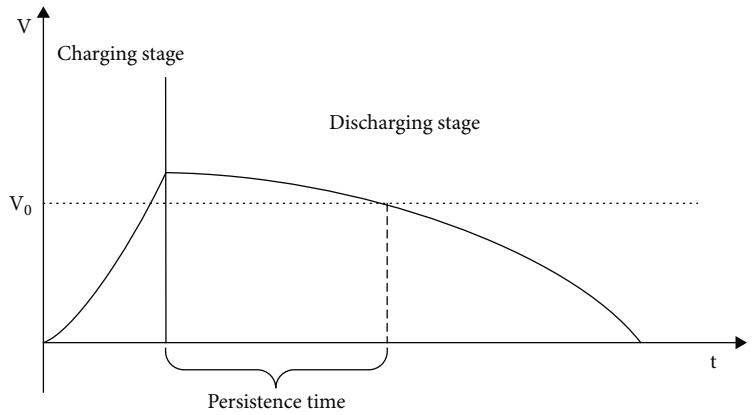


Figure 1: Persistence time.

threshold V_0 is defined as the "persistence time" [19]. Figure 1 shows the persistence time of tag charging and discharging. During this time, the tag's internal capacitive power supply continuously charges the internal volatile memory, maintaining its internal data. According to the EPCglobal Gen 2 standard, the time of the process from charging to the full charge of the tag is no more than 2 ms [3, 4]. The inventory flag under the four sessions and the SL flag are kept by the tag's internal volatile storage area. They will be lost due to power outages and reverting to the default state (state A or state $\sim$SL) upon the power supply. Chen et al. [19] propose various methods to measure the tag charging duration using this property. To capture the tag's persistence time efficiently and accurately, we present an optimized method for stepwise capturing persistence time.

3.3. Unauthorized Readers Behavior. This subsection analyzes the reading behavior of unauthorized readers. The core parameters of the Query command mainly have three parameters: Session, Target, and Sel, which control the session used in this round, the state of the tag, and the tag SL flag, respectively. For example, the command Query : {Session = 2, Target = A, Sel = $\sim$SL} is to query the tags with state A under Session 2 and Selected Flag $\sim$SL. Since the Sel parameter can be ignored, we perform a Cartesian product combination of Session and Target to obtain the full read pattern of the reader, as shown in Table 3.

Table 3: Unauthorized readers' behaviors.

Num	Session	Target
1	0	A
2	0	B
3	1	A
4	1	B
5	2	A
6	2	B
7	3	A
8	3	B

4. URDTE Overview

4.1. Basic Idea. The core idea of detecting unauthorized readings is to detect whether there is an unauthorized reader to access (charge) the tag by taking advantage of the tag's feature of sustained power after charging. The core detection process of URDTE is divided into three parts: first, we start the reader and launch the radio frequency signal to charge the tag. Second, we close the reader to stop the signal transmission. Third, we check the tag's power status after waiting for t_{gap} seconds. t_{gap} is the time it takes for the tag to run out of power. If the tag still has the remaining power after the t_{gap}, it means that unauthorized readers have carried out the charging process to the tag. It is not easy to detect the voltage and current information of the internal capacitance

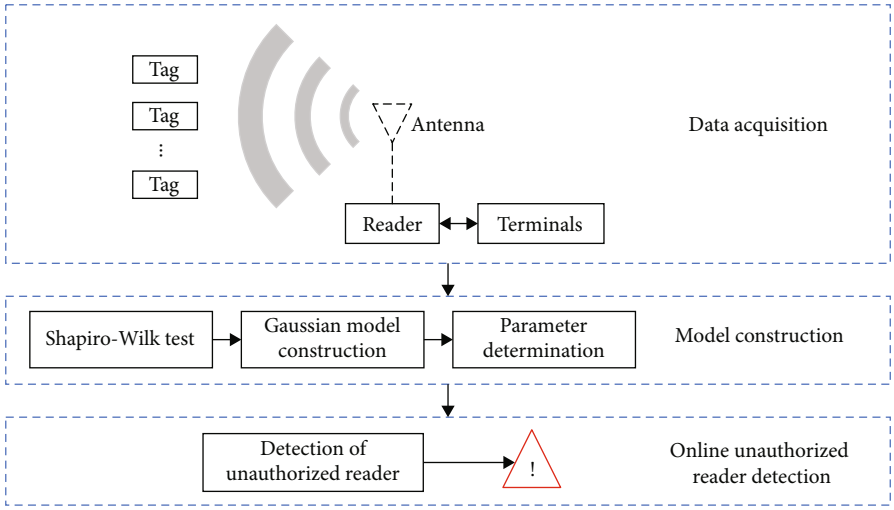


Figure 2: Framework of URDTE.

of the tag. We use the concept of persistence time to measure the ability of the tag to store power internally and use the inventory flag defined in the EPCglobal Gen 2 standard to detect whether the tag is in a state of power. The tag's electrical energy can be obtained by flipping this flag and continuously checking its status.

In practical implementation, selecting the waiting interval t_{gap} has a decisive influence on the detection performance. The best choice for t_{gap} is to make it consistent with the actual persistence time of the tag. In theory, the persistence time of a tag is only related to the capacitive circuitry inside the tag and is a stable value. However, when we collect the persistence time of the tags, the data collected each time will be slightly different. The model of the reader and external factors during the acquisition process will slightly affect the accuracy of the persistence time. To eliminate the effects caused by random factors during the acquisition process, we collected persistence time several times and constructed a Gaussian model to describe persistence time as accurately as possible to select the optimal waiting interval t_{gap}.

4.2. URDTE Overview. The unauthorized reader detection method based on the tag's energy consists of three main phases. Figure 2 shows the general framework of URDTE.

The first phase is the data acquisition. This part collects the persistence time of the tag for subsequent modeling. It mainly includes the tag attached to the object, the reader reading the tag, the antenna to transmit the RF signal, and the terminal to handle the collected data.

The second phase is the model construction. In this phase, to cope with the variability of the actual environment, a distribution test of the collected persistence time data is required before the Gaussian model is constructed. By counting the data collected in the previous phase and using the Shapiro-Wilk test, we test whether the collected persistence time data conformed to the Gaussian distribution. If they do not match, we return to the first stage for data collection again. If they match, we accept this data and use it to construct a Gaussian model. After constructing the Gaussian model, we calculate the tolerance factor Δt to estimate the minimum discharge time. The false negative rate will increase when increasing Δt. Whereas Δt decreases, the false positive rate will increase. Therefore, the determination of Δt is critical. We will provide a detailed theoretical analysis of the selection of Δt.

The last phase is the online unauthorized reader detection stage, which is the core part of URDTE. In this phase, the reader carries on the charge to the tag. After waiting for the predicted time when the tag power should be exhausted, it detects whether the tag power is exhausted. If it detects the tag still has the remaining power, it indicates that the tag is read by the unauthorized reader and has completed the charging process. URDTE keeps repeating the above process to judge whether there is an unauthorized reader.

5. URDTE Design

5.1. Data Acquisition. The first module of the URDTE is the data acquisition module, whose primary function is to collect the persistence time of the tag. The primary basis for the persistence time collection is the change of the tag's inventory flag. The tag's inventory flag is stored in an internal volatile memory area, which causes the tag to lose inventory flag data when the battery is depleted and automatically reset to its initial state when recharging. As we introduced in Section 3, there are four session modes within the tag, each with its independent flag, and the flag exists in two states, *A* or *B*. The default state is *A*. Therefore, we can first set the tag inventory flag to *B*. After waiting for t_{gap} seconds, the Query command is used to inventory the tag in state *B*, and if a tag response is received, it means that the tag is still in state *B*, i.e., there is still power to maintain its inventory flag. Keep increasing t_{gap} until there is no tag response, where t_{gap} is the persistence time of the tag.

The selection of the time interval t_{gap} is crucial. We use a stepwise approach to collect it. The specific approach is to

Input: Whether the Query command get tags: True or False
Output: The persistence time: pt
s = rand (2 or 3)
step =1//the step value in current iteration
pt =0//the persistence time
t_{gap} =1//the waiting time in this round
While step > 0.01 **do**
  Reader: Select(session = s, action = 100_2)
  Stop the reader
  Sleep t_{gap}
  If reader: Query(session = s, target = B, Sel = 00_2)
  Get tags **then**
    $t_{gap} = t_{gap}$ + step
  Else
    pt = t_{gap} − step
    step = step ∗ 0.1
  End if
End while
Return pt

Algorithm 1:Persistence time acquisition algorithm.

use a large granularity time interval to collect rough persistence time in the initial stage, lock the range, and then gradually reduce the time granularity. The specific algorithm pseudocode is shown in Algorithm 1.

5.2. Model Construction. This section introduces the construction of the detection model with three core parameters: the Gaussian model of the persistence time, the maximum persistence time $PT_{\max}$, and Δt. First, we perform Gaussian model using the persistence time. Then, the Shapiro-Wilk test is used to check whether the data conforms to the Gaussian distribution [20]. Finally, we describe the determination of parameters Δt.

5.2.1. Shapiro-Wilk Test. The Shapiro-Wilk test tests the null hypothesis that a sample $\{\mathrm{pt}_1, \cdots, \mathrm{pt}_n\}$ comes from a normally distributed population. We use n to denote the amount of persistent time data. First, we arrange the collected persistence time in order.

$$\mathrm{pt}_1 \le \mathrm{pt}_2 \le \cdots \le \mathrm{pt}_i \le \cdots \le \mathrm{pt}_n. \tag{1}$$

Then, we calculate the value of the statistic W according to Formula (2).

$$W = \frac{\left(\sum_{i=1}^{(n/2)} a_i (\mathrm{pt}_{n+1-i} - \mathrm{pt}_i)\right)^2}{\sum_{i=1}^{n} (\mathrm{pt}_i - \bar{\mathrm{pt}})^2}. \tag{2}$$

The coefficients a_i are given by

$$(a_1, a_2, \cdots, a_n) = \frac{m^T V^{-1}}{C}, \tag{3}$$

where C is a vector norm,

$$C = \left|V^{-1} m\right| = m^T V^{-1} m^{(1/2)}, \tag{4}$$

and the vector m,

$$m = (m_1, \cdots, m_n)^T, \tag{5}$$

where m is constructed from the anticipated values of the order statistics of independently distributed random variables selected from the standard normal distribution, and V is the covariance matrix for those statistics.

Finally, we obtain the critical value W_α at the significance level $\alpha = 0.1$ and compare the magnitude of the calculated W with the critical value W_α. If $W \ge W_\alpha$, then the original data conform to the normal distribution. Otherwise, it is necessary to return to the acquisition phase to recollect the persistence time.

5.2.2. Gaussian Model Construction. When the persistence time $\mathrm{PT} = \{\mathrm{pt}_1, \cdots, \mathrm{pt}_n\}$ accords with a Gaussian distribution, it can be expressed as follows:

$$\mathrm{PT} \sim N(\mu, \sigma^2). \tag{6}$$

The mean of the persistence time data can be expressed as

$$\mu = \frac{1}{n} \sum_{i=1}^{n} \mathrm{PT}_i. \tag{7}$$

In addition, we also need to record the maximum data $PT_{\max}$ in the persistence time data sample, which determines the waiting time t_{gap} together with the tolerance factor Δt.

5.2.3. Parameter Determination. In order to better describe the setting of Δt, Figure 3 shows the model of the tag state changing with time. The tag state is set to B and the SL state is set to positive at t_1 and reaches time t_3 after T_{gap} seconds have elapsed. The algorithm detects whether there is a tag

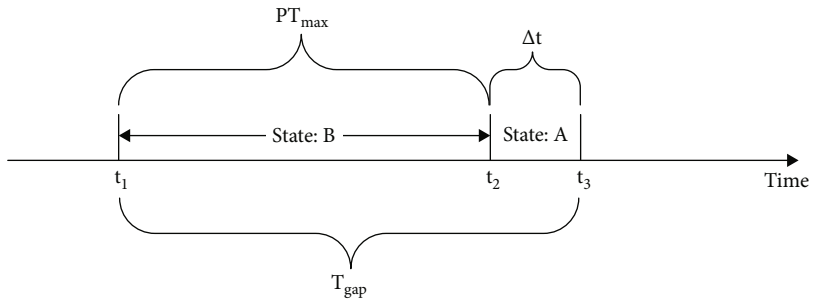


Figure 3: Model of tag state.

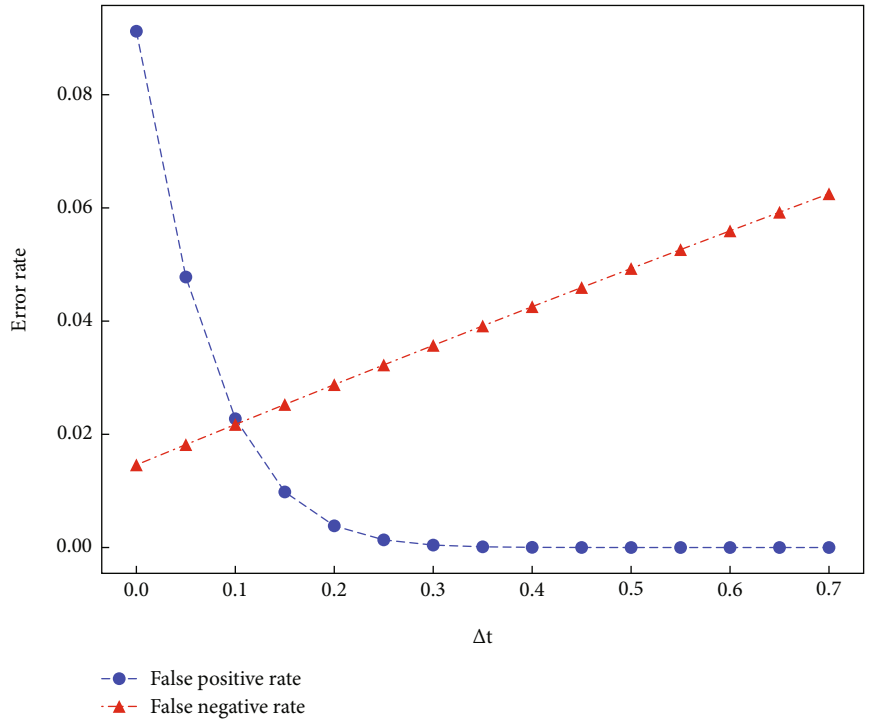


Figure 4: Tolerance factor Δt setting.

with state B at this time. After detecting that there is no tag with state B, it detects whether there is a tag with state SL as positive. If the tag power is not consumed at t_3, it will cause false positives. The setting of the tolerance factor Δt ensures that the tag power has been exhausted.

The probability of false positive alarm prob_{FP} caused by the tag's power not being consumed at t_3 is

$$\text{prob}_{\text{FP}} = P(\text{PT} > \text{PT}_{\max} + \Delta t). \tag{8}$$

However, if Δt is too large, it will lead to a longer t_{gap} and affect the detection accuracy. For example, the unauthorized reader reads the tag immediately after t_1. Due to the long t_{gap}, although the tag is read by an unauthorized reader and completes charging during this process, it may still run out of power before the detection at t_3, resulting in a missed alarm. That is, if an unauthorized reader reads within the time range of $(t_1, t_3 - \text{pt})$, it will run out of power before the detection at t_3. The probability of a false negative prob_{FN} in this case is

$$\text{prob}_{\text{FN}} = \frac{(\text{PT}_{\max} + \Delta t) - \mu}{\text{PT}_{\max} + \Delta t}. \tag{9}$$

To strike a balance between the two false alarm rates, we take the intersection of the false negative rate curve and the false positive rate curve as the value of Δt, as shown in Figure 4.

Therefore, we use the following equations to solve the Δt.

$$\begin{cases} \text{prob}_{\text{FP}} = P(\text{PT} > \text{PT}_{\max} + \Delta t), \\ \text{prob}_{\text{FN}} = \dfrac{(\text{PT}_{\max} + \Delta t) - \mu}{\text{PT}_{\max} + \Delta t}, \\ \text{prob}_{\text{FP}} = \text{prob}_{\text{FN}}. \end{cases} \tag{10}$$

Input: The maximum value of the persistence time: PT_{max}
Tolerance factor: Δt
Output: The result of unauthorized reader detection: res
s = rand (2 or 3)
$T_{gap} = PT_{max} + \Delta t$
While True **do**
  Reader:Select(session = s, action = 001_2)
  Reader:Query(session = s, Target = A, Sel = 00_2)
  Stop the reader
  Sleep t_{gap}
  If reader:Query(session = s, target = B, Sel = 00_2)
  Get tags **then**
    res = True
  Else if reader:Query(session = s, target = A, Sel = 11_2) get tags **then**
    res = True
  Else
    res = False
  End if
  If res = True **then**
    Return res and alarm
  Else
    Return res
  End if
End while

Algorithm 2: Unauthorized reader detection algorithm.

5.3. Unauthorized Reader Detection. The basic idea is that the tags are inventoried (charged) at regular intervals, and after a specific interval, the tags are checked to see if they have been inventoried (charged) during this interval. We found that the state under *S*2 and *S*3 sessions in the tag, as well as SL, rely on the power saved by the capacitor inside the tag to maintain its state and will revert to the default state after the tag runs out of power. We detect whether an unauthorized reader accesses the tag through the state change of these flags. The steps are as follows:

(1) Start the reader, adopt the Select command to change the tag status under Session 2 to state *B*, and state SL is set to positive, finish charging, and stop the reader

(2) After waiting for T_{gap} seconds, use the Query command to query whether there is a tag with Session 2 state *B*. If a tag response exists, it indicates the presence of the unauthorized reader. Otherwise, continue to the next step

(3) Use the Query command to query whether there is a tag whose SL flag is true to indicate the presence of an unauthorized reader

When the unauthorized reader adopts *S*0, *S*1, or *S*3 session to carry on the tag inventory (unauthorized reader mode as 1-4, 7-8 in Table 3), it will charge the tag and directly increase the tag's flag persistence time after successfully communicating with the tag. Therefore, it can be detected by step 2.

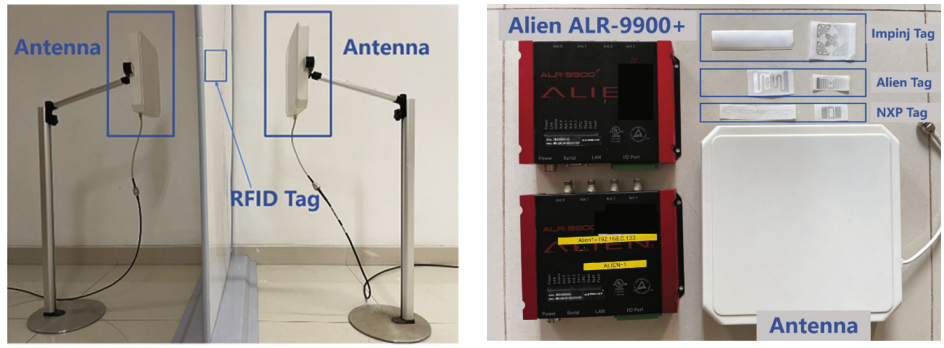
When an unauthorized reader uses an *S*2 session for unauthorized reading (unauthorized reader mode is 5-6 in Table 3), since the unauthorized reader uses the same session as the legal reader, this affects our flag state and needs to be discussed in detail. On the one hand, when the unauthorized reader adopts the *S*2 session and reads the tag of state *A* (unauthorized reader mode corresponds to 5 in Table 3), the tag will not respond because the tag state has been modified to state *B*. However, since other Query commands charge the tag, this read increases the persistence time of the tag. On the other hand, when the unauthorized reader uses the *S*2 session and reads the tag in state *B* (the unauthorized reader mode corresponds to 6 in Table 3), the unauthorized reader can successfully read the tag because the tag state has already been modified to state *B*, and the tag state is automatically flipped to state *A* at this time. The second step of URDTE cannot effectively detect this situation because it will query the tag of state *B*, and if there is no state *B* tag, it is considered that there is no unauthorized reader. This situation needs to go to the third step to detect.

The third step detects the SL flag. Although the unauthorized reader mode 6 uses the same session with legal readers, the read operation does not affect the SL flag so that the unauthorized reader mode 6 can be detected accurately.

In addition, we can randomly choose to use *S*2 or *S*3 to enhance the randomness of the detection algorithm and reduce the probability of collision with the read session used by unauthorized readers. The pseudocode for the detection process is shown in Algorithm 2.

6. Device Deployment and Experimental Result

In this section, we implement a prototype of URDTE in a commodity RFID system. Besides, we evaluate the performance of



(a) (b)

Figure 5: Experimental scene. (a) System prototype. (b) Equipment and tags.

URDTE through extensive experiments in terms of robustness to environmental changes and detection accuracy.

6.1. System Deployment. The system prototype is shown in Figure 5(a), where the equipment and tags used are shown in Figure 5(b). The reader used in the system is Alien ALR-9900+, and the tags of three manufacturers are selected: Impinj, Alien, and NXP. We follow LLRP [21] (Low-Level Reader Protocol for EPCglobal Gen 2 standard) for reader development and do not need to make any changes to the reader hardware or firmware. The back-end computer is equipped with an Intel Core i5-8250U 1.6 GHz CPU and 8 GB RAM.

6.2. Detection Performance. In the experiment, we tested the influence of tag chip, angle, power, and distance of unauthorized reader on URDTE detection effectiveness. The detection of unauthorized readers is essentially a binary classification problem. Therefore, we evaluate URDTE using classical metrics from machine learning. Our prototype system feeds back the detection results at a fixed frequency with positive or negative to indicate the presence of unauthorized readings. There are four cases as follows:

(1) If there is an unauthorized reader intrusion, and URDTE detects this intrusion, it is a true positive (TP)

(2) If there is an unauthorized reader intrusion, but it is not detected by URDTE, it is a false negative (FN)

(3) If there is no unauthorized reader intrusion, and URDTE feedback results in a normal state, it is a true negative (TN)

(4) If there is no unauthorized reader intrusion, but URDTE feedback results in unauthorized reader intrusion, that is a false positive (FP)

False positive (FP) and false negative (FN) in these misclassifications are our focus, where false positive (FP) can cause false alarms, while false negative (FN) can cause missed alarms for intrusions, resulting in a security risk. In addition, the accuracy rate is also the focus of our attention. Therefore, we will use these three metrics to evaluate the effectiveness of the prototype system, which are defined as follows:

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{TN} + \mathrm{FP}}, \tag{11}$$

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{TN} + \mathrm{FP}}, \tag{12}$$

$$\mathrm{Accuracy} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TN} + \mathrm{FP} + \mathrm{FP} + \mathrm{FN}}. \tag{13}$$

6.2.1. Effect of Tag's Chip on Accuracy. UHF RFID reader and tag follow the specifications of the EPCglobal Gen 2 protocol for communication. Although the EPCglobal Gen 2 protocol specifies that the tag should have four communication sessions, the requirements for session 2 and session 3 are vague and only require a persistence time greater than 2 seconds. Through experiments, we found that different brand tags' persistence times are different, even if the chips of different models of the same brand are different. Therefore, we tested different tag chips for their accuracy.

We, respectively, place each kind of tag 0.5 meters directly in front of the legal reader, and the unauthorized reader antenna is placed at 0.5 meters at the back of the tag, and carry out 500 times unauthorized reading for each kind of tag, respectively.

The results are shown in Figure 6. The detection accuracy of all tags was high (>97%), and the false negative rate was low (<3%), indicating that URDTE has a high detection rate and is not affected by the tag chip type.

6.2.2. Effect of Tag Angle on the Accuracy. We place the tag at 0.5 meters in front of the legal reader and change the angle between the tag and the reader. We set the angle between the tag and the legal reader antenna to 0, 45, 90, 135, 180, 225, and 270, respectively. The unauthorized reader performs illegal readings in front of the tag 500 times for each angle separately.

The experimental results are shown in Figure 7. At the 90 and 270, the RF signal emitted from the antenna cannot successfully activate the tag due to the specificity of the angle, resulting in the system not being able to read the tag, i.e., the charging process of the tag cannot be completed.

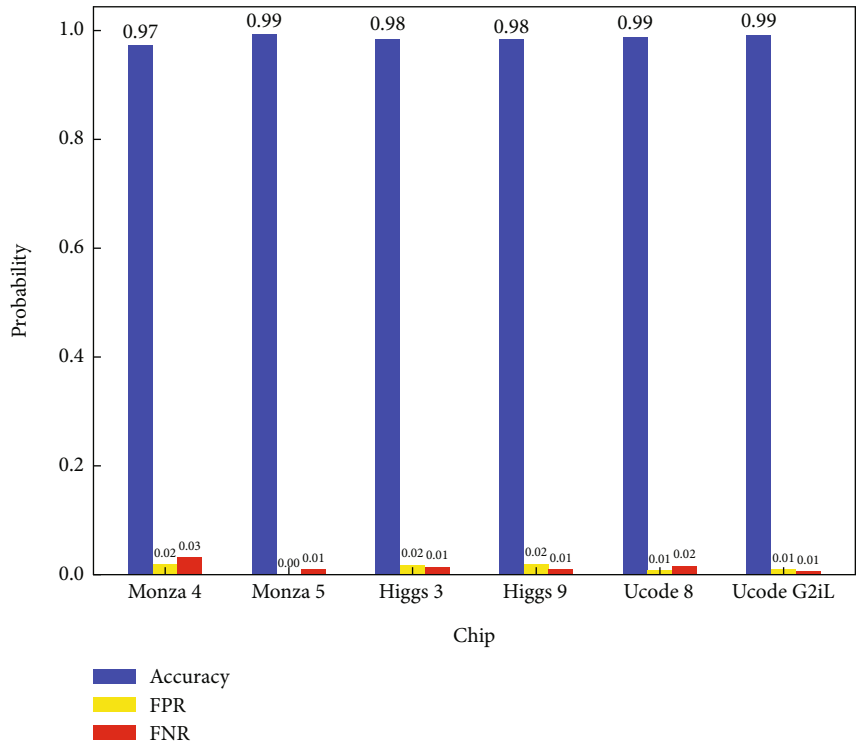


Figure 6: Different chips.

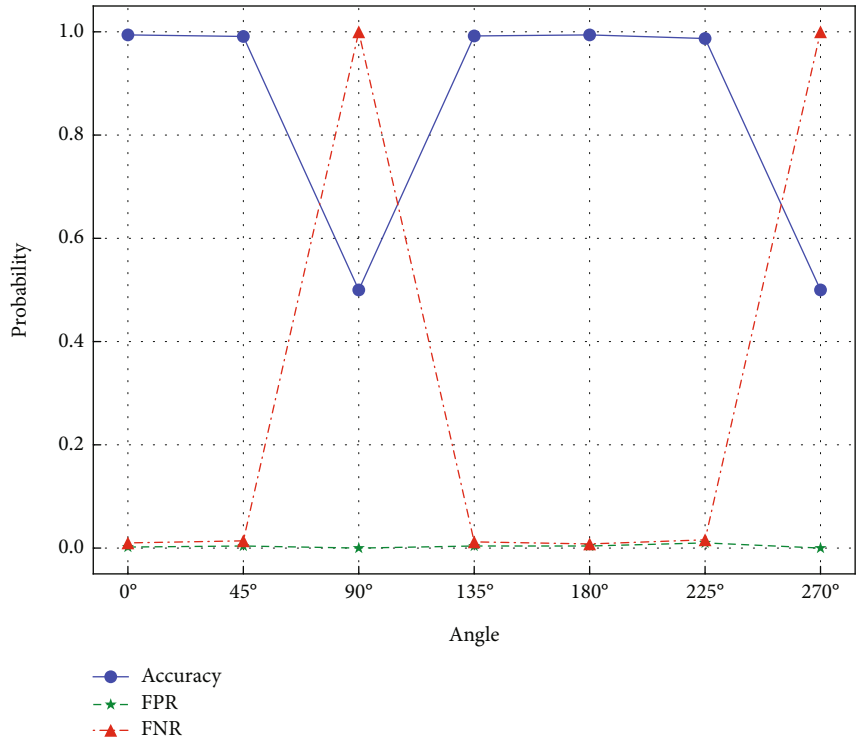


Figure 7: Different angles.

For the other angles, it can be found that the error rate and accuracy do not change much with the change of angle, and both have good detection results. Therefore, when we deploy and apply the system, we should pay attention to the legal antenna should try to form a parallel angle with the tag to get the best detection effect, and if the tag signal is found to disappear during the detection process, the angle between the tag and the antenna should be adjusted appropriately.

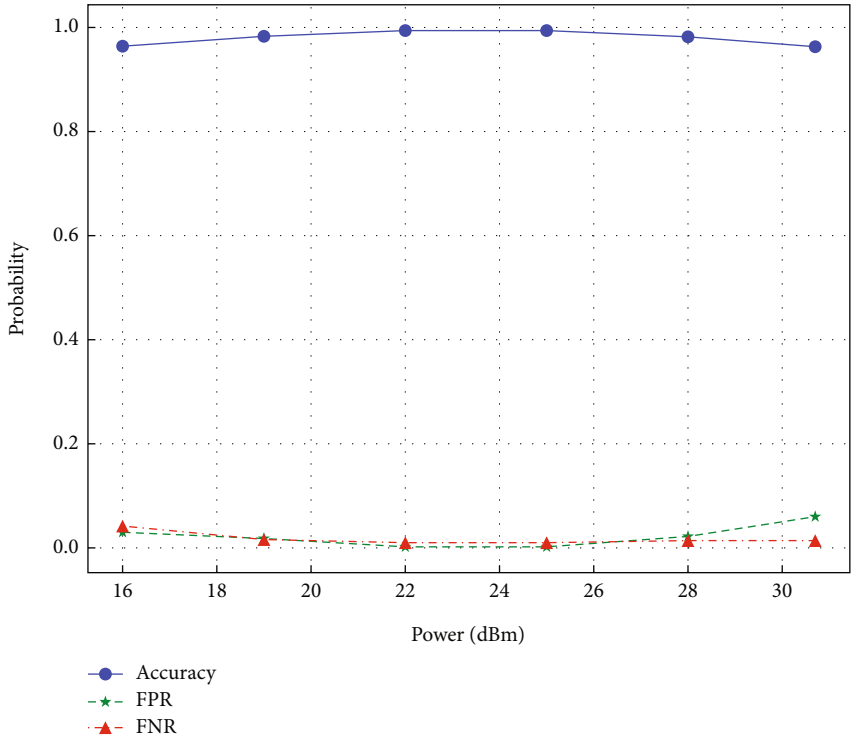


Figure 8: Different power.

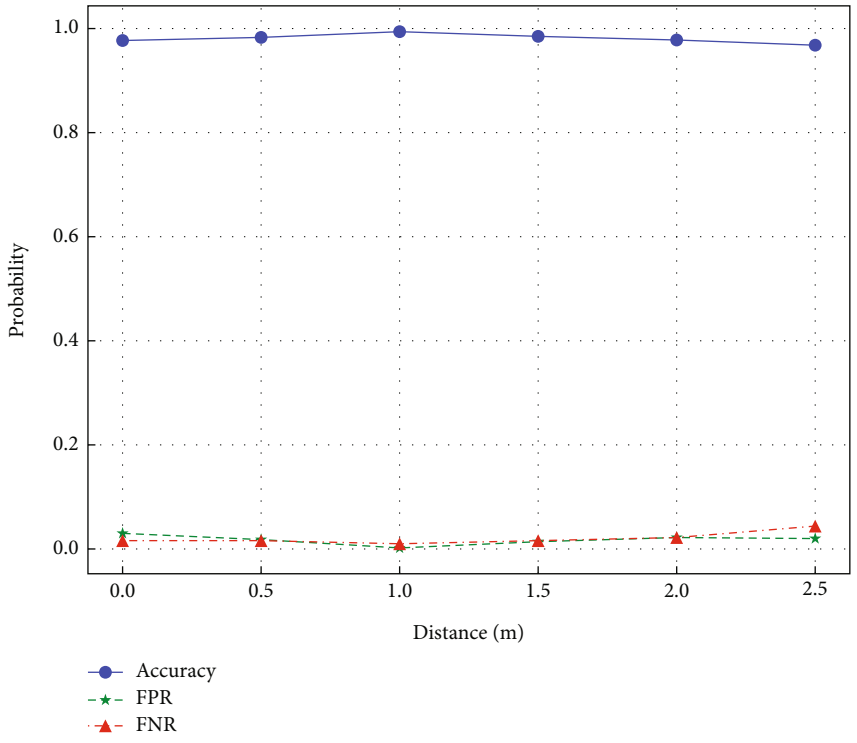


Figure 9: Different distances.

6.2.3. Effect of Unauthorized Reader Power on Accuracy. In this experiment, we investigate the effect of unauthorized reader transmit power on detection accuracy. We place the tag between legal and unauthorized readers, and the tag is 0.5 meters away from both legal and unauthorized readers. Unauthorized readers perform unauthorized readings from16 dBm to 30 dBm. The experimental results are shown in Figure 8. We found that the detection accuracy will be

high at the appropriate power. However, the detection accuracy will be suppressed to a certain extent under small or large power. The results show that the URDTE can detect the intrusion with high accuracy regardless of the power of the unauthorized reader.

6.2.4. Effect of Unauthorized Reader Distance on Accuracy. In this experiment, we move the unauthorized reader and change the distance between the unauthorized reader and the tag to investigate the effect of distance on the detection accuracy. We first place the unauthorized reader at a distance of 2.5 meters from the tag and constantly reduce the transmit power of the unauthorized reader. We found that when the power is less than 18 dBm, the unauthorized reader will no longer read the tag. We deliberately set the transmit power of the unauthorized reader to 18 dBm. That is, at 2.5 meters, 18 dBm is the minimum power to be able to read the tag. We keep the distance between legal readers and tags at 0.5 meters, then move unauthorized readers to distances of 0, 0.5, 1, 1.5, 2, and 2.5 meters from the tags for testing and perform 500 reads at each distance.

Figure 9 shows that even if the unauthorized reader performs unauthorized reading at low power at a remote location, our system can still accurately detect this intrusion and still has a high accuracy rate. Regardless of the distance and the power of the unauthorized reader, as long as the unauthorized reader can read the tag, it will complete the charging of the tag, which makes our detection method extraordinarily stable and robust. However, if the distance is too large or too small, it will slightly impact the detection accuracy. The reason is that the charging and discharging times of the tags are slightly different at different distances.

In summary, the experimental results show that the URDTE algorithm has extremely high detection accuracy and robustness for unauthorized readers with different chips, powers, and distances on the premise that legal readers can read tags. Moreover, the algorithm does not rely on special detection equipment. The detection method is low cost and has high practical application value for discovering unauthorized readers and protecting the security of air interface data of the RFID system.

7. Conclusion

This paper proposes a method for detecting unauthorized reading based on the tag's power. The core idea of this method is to determine whether an unauthorized reader has accessed a tag by detecting the tag power. We implemented this method on a commercial reader following the EPCglobal Gen 2 standard. Extensive experiments have shown that URDTE has high accuracy and strong robustness in detecting unauthorized reading, and this method effectively enhances RFID system security, which is essential for preventing air interface intrusion.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Strategic Priority Research Program of Chinese Academy of Sciences, Grant No. XDC02040300.

References

[1] K. Domdouzis, B. Kumar, and C. Anumba, "Radio-frequency identification (RFID) applications: a brief introduction," *Advanced Engineering Informatics*, vol. 21, no. 4, pp. 350–355, 2007.

[2] Y. Ye, L. Shi, X. Chu, and G. Lu, "On the outage performance of ambient backscatter communications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7265–7278, 2020.

[3] E. O. R. Implied, T. This, D. Is et al., *Specification for RFID Air Interface EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 Mhz 960 Mhz*, 2008.

[4] EPCglobal, *Epc Radio-Frequency Identity Protocols Generation-2 UHF RFID Standard, Specification for RFID Air Interface Protocol for Communications at 860 Mhz960 Mhz*, 2018.

[5] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, Special Publication 800-98, National Institute of standards and Technology, Technology Administration U.S. Department of Commerce, 2007, http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf .Accessed15.

[6] H. Y. Chien, "Sasi: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Computer Society Press*, 2007.

[7] Q. Jia, P. Chen, X. Gao, L. Wei, and B. Zhao, "Lightweight anti-desynchronization RFID mutual authentication protocol," *Journal of Central South University(Science and Technology)*, vol. 46, no. 6, pp. 2149–2156, 2015.

[8] Z. Rong, L. Zhu, X. Chang, and Y. Yi, "An efficient and secure RFID batch authentication protocol with group tags ownership transfer," *Collaboration and Internet Computing*, 2015.

[9] A. Razm and S. E. Alavi, "An intrusion detection approach using fuzzy logic for RFID system," *Advances in Information Science and Applications*, vol. 2, 2014.

[10] H. Ding, J. Han, Y. Zhang et al., "Preventing unauthorized access on passive tags," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pp. 1115–1123, Honolulu, HI, USA, 2018.

[11] Y. Zhang, L. T. Yang, and J. Chen, *RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations*, CRC Press, 2009.

[12] M. V. D. Burmester and J. Munilla, "Lightweight RFID authentication with forward and backward security," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–26, 2011.

[13] Q. Qian, Y.-L. Jia, and R. Zhang, "A lightweight RFID security protocol based on elliptic curve crytography," *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361, 2016.

[14] K. Fan, N. Ge, Y. Gong, H. Li, R. Su, and Y. Yang, "An ultra-lightweight RFID authentication scheme for mobile commerce," *Peer-topeer Networking and Applications*, vol. 10, no. 2, pp. 368–376, 2017.

[15] D. Ma and N. Saxena, "A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems," *Security and Communication Networks*, vol. 7, 2695 pages, 2014.

[16] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM conference on Computer and communications security*, pp. 103–111, New York, NY, USA, 2003.

[17] W. Zhang, S. Zhou, J. Luo, H. Cheng, and Y. Liao, "A lightweight detection of the RFID unauthorized reading using rf scanners," in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, pp. 317–322, New York, NY, USA, 2015.

[18] D. Sun, Y. Cui, Y. Feng, J. Xie, S. Wang, and Y. Zhang, "Urtracker: unauthorized reader detection and localization using cots RFID," in *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 339–350, Cham, 2021.

[19] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: robust energy-related fingerprinting for passive {RFID} tags," *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*, pp. 1101–1113, 2020.

[20] S. S. Shapiro and M. B. Wilk, "An analysis of variance test for normality (complete samples)," *Biometrika*, vol. 52, no. 3-4, pp. 591–611, 1965.

[21] GS1, *Low level reader protocol*, 2008, https://www.gs1.org/standards/epc-rfid/llrp/1-1-0.